

开源生态白皮书

（2020 年）

中国信息通信研究院
2020年10月

前　言

近几年开源技术快速发展，在云计算、大数据、人工智能等领域逐渐形成技术主流，开源技术已经成为企业构建信息系统的重要选择，国内企业参与开源生态的热情度持续提升。

本白皮书是中国信息通信研究院在开源领域发布的白皮书，分析国内外开源生态发展现状，梳理当前发展热点，展望未来发展趋势。白皮书首先介绍了开源生态发展概况，重点围绕开源布局、开源运营、开源治理、开源风险、行业开源等开源领域热点话题进行探讨，最后对开源生态未来发展进行了展望。

目 录

图 目 录

表 目 录

一、开源生态概述

（一）开源概念逐渐明晰

开源既是一种协作模式，也是一种特性的产品。开源形态最早出现于上世纪六十年代，软件代码附属硬件产品以开源的形式分发。1983 年，Richard Matthew Stallman 发起 GNU 计划，推动自由软件概念，成为开源软件早期形态。开源软件明确定义由 1998 年 OSI 给出，包括十大特性，即自由再发布、源代码公开、允许派生作品、作者源代码完整性、不能歧视任何个人或团体、不能歧视任何领域、许可证的发布、许可证不能只针对某个产品、许可证不能约束其他软件、许可证必须独立于技术。

从过程维度看，开源是一种分布式协作模式，从结果维度看，开源是一种特定形态的产品，具有公开、可使用、可修改、可分发特点。开源软件比自有软件更宽松，开源软件与免费软件无直接对应关系，公开代码不一定是开源软件。

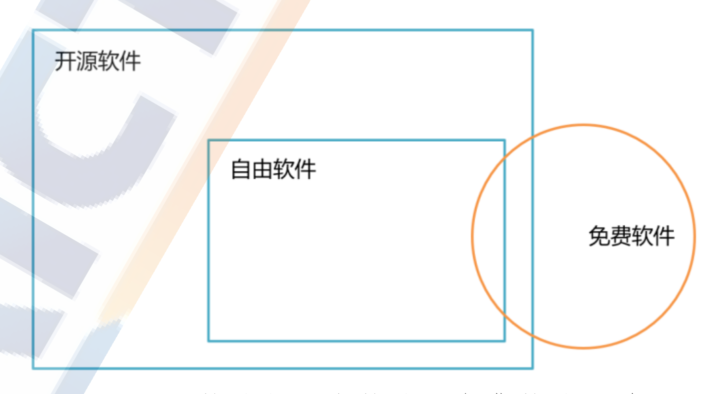


图 1 开源软件与自由软件、免费软件的关系

开源生产模式逐渐成为新一代软件开发模式。随着产业数字化发展，信息技术需要满足业务场景发展需求，具有海量数据处理能力，

快速上线迭代特点，多场景异构兼容性，传统软件封闭开发模式在创新度、迭代速度上均存在一定限制。开源开发模式具有公开透明的特点，有效聚集优质开发人员，形成分布式协作，推动产品快速迭代，同时丰富企业商业模式，促进科技公司良性竞争。

（二）开源生态以开源项目为中心构建

开源生态以开源项目为中心构建，依托开源社区协作形成软件、硬件等开源项目。涉及开源贡献者、开源使用者、开源运营者、开源服务者多重角色，包含开源治理、开源运营、开源商业布局等多个环节，需要满足开源规则要求，依托代码托管平台等基础设施构建。

微观层面开源生态依托四大角色进行有效协作。开源生态涉及开源贡献者、开源使用者、开源运营者、开源服务者等多个角色，企业和个人均可参与。开源贡献者主要最初贡献开源项目的企业或个人，目前以科技公司贡献为主；开源使用者指开源的使用主体，涉及范围广泛；开源运营者主要指促进开源协作的主体，开源基金会项目托管是一种成熟的开源运营模式；开源服务者指基于开源提供商业产品或服务的企业。对于开源贡献者和开源服务者，开源是实现商业布局的一种途径，可将开源布局与商业产品布局进行有效结合，推动用户使用，在应用层面有效降低边界成本，扩大用户使用范围。对于开源使用者，开源模式推动产品快速迭代，激发产品创新，丰富产业侧供应体系，建立用户需求联动机制。

宏观层面开源生态涉及开源运营、开源治理、开源商业布局、开源规则、基础设施等多个要素。开源运营推动开发者持续贡献开源项

目，推动开源项目在产业用户中的使用；开源治理是针对开源引入过程、自发开源过程、开源社区维护等方面的一套流程体系，是推动开源生态良性发展的有效手段；开源商业布局是将开源与自身商业模式进行有效结合，实现商业转换的过程；开源规则包括法律环境、开源社区规定、开源许可证等，明确开源使用分发的权利义务；开源基础设施包括开源代码托管平台、社区网站等，支撑开源协作。

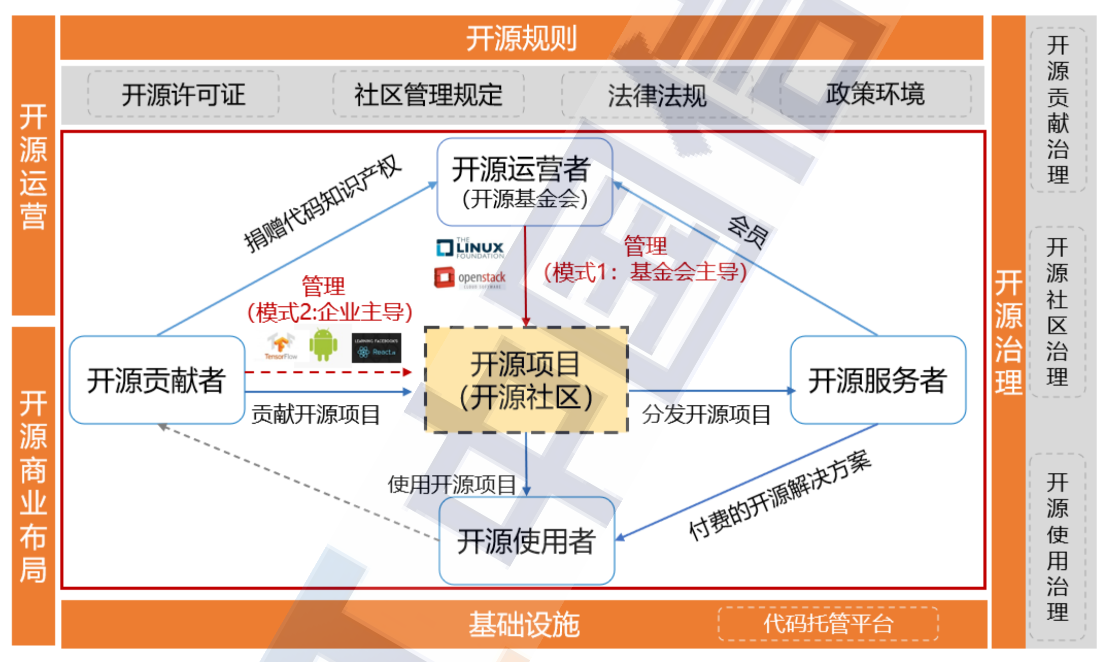


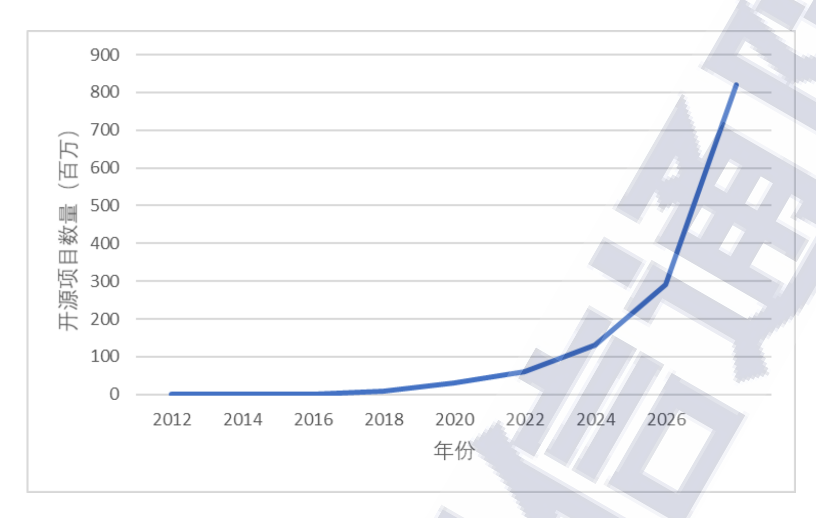
图 2 开源生态架构图

二、开源生态发展现状

（一）开源数量持续攀升，我国开源覆盖全栈技术领域

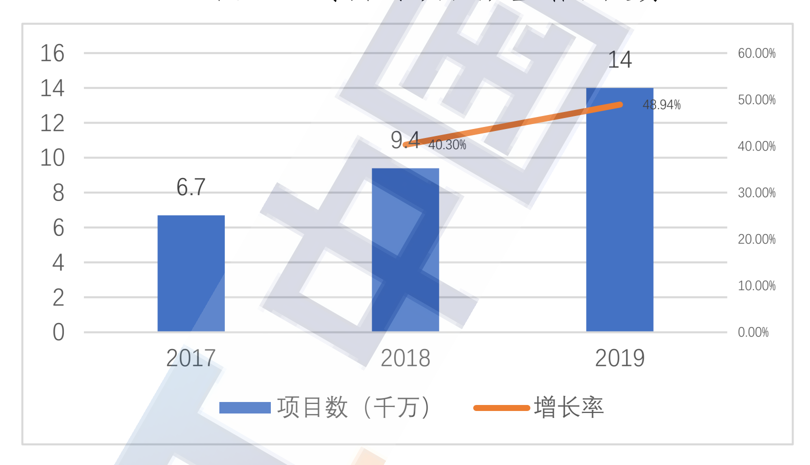
全球开源项目数量呈指数级增长。根据全球最大开源代码托管平台GitHub年度报告数据显示，截至2019年GitHub托管仓库已有1.4亿，2019年新增仓库4400万个，创建第一个项目的用户比2018年增加44%，

130万开发者对开源做出首次贡献。SourceClear调查报告指出开源项目已呈现指数级增长趋势，2026年预计超过3亿。



数据来源：SourceClear 调查报告

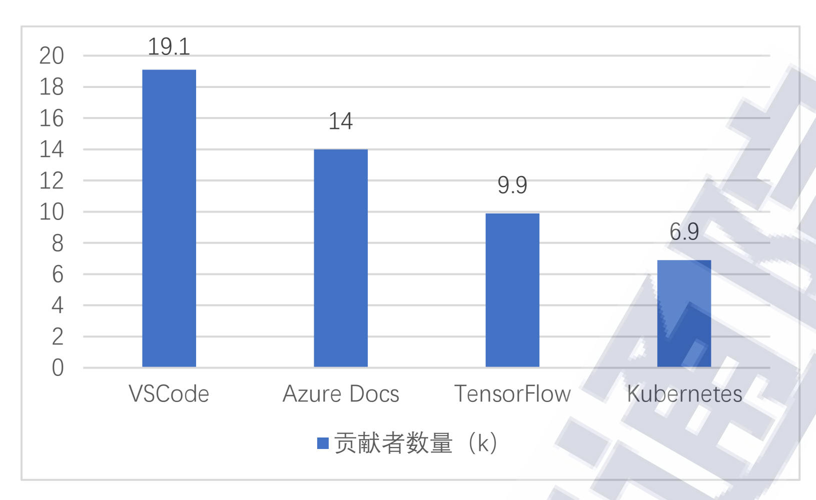
图 3 全球开源项目数量增长趋势



数据来源：GitHub，2019年11月

图 4 GitHub 近三年开源项目数量及增长率

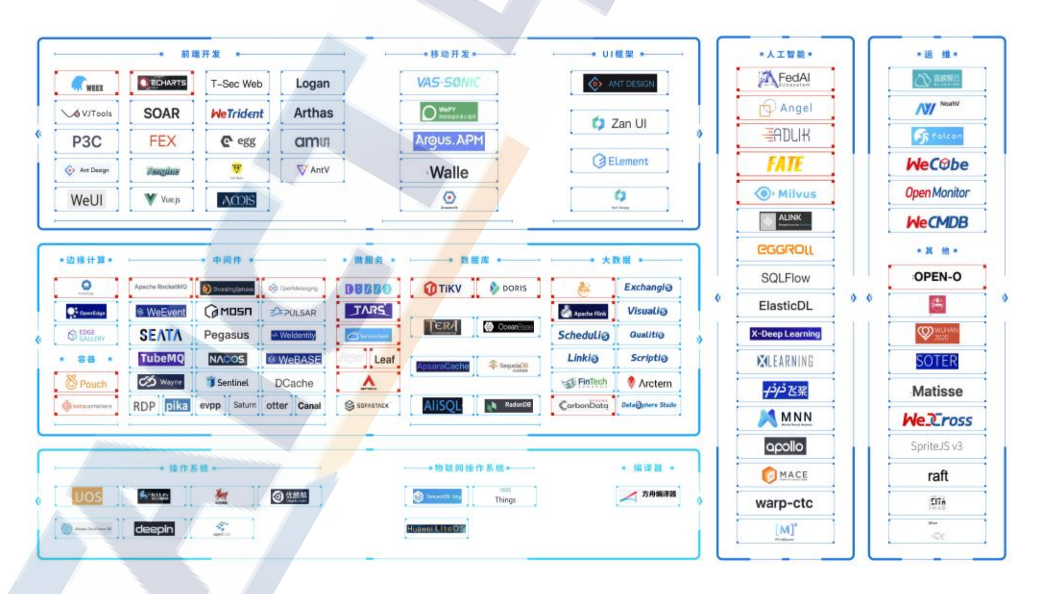
活跃开源项目集中在新兴技术领域。2019年GitHub代码仓库中，人工智能、云计算等新技术领域开源项目关注度较高，微软的源码编辑器VSCode、机器学习文档Azure Docs是2019年GitHub上贡献者最多的开源项目，其次是谷歌的机器学习平台TensorFlow、容器编排平台Kubernetes和Facebook的移动应用开发框架React Native框架。



数据来源：GitHub，2019年11月

图 5 全球开源项目贡献者数量

我国自发开源项目覆盖全栈技术领域。我国自发开源项目涵盖底层操作系统、物联网操作系统和编译器，中间层边缘计算、容器、中间件、微服务、数据库和大数据，上层前端开发、移动开发和UI框架，另外还有人工智能领域、运维和其他热门开源项目，基本覆盖目前主要的技术领域，接近30个的开源项目已经捐赠给开源基金会，走向国际。



数据来源：中国信息通信研究院，2020 年 6 月

备注：红框代表开源项目捐赠给开源基金会

图 6 中国自发开源项目分布地图

（二）开源占据各领域主要市场份额，我国开源应用逐年攀升

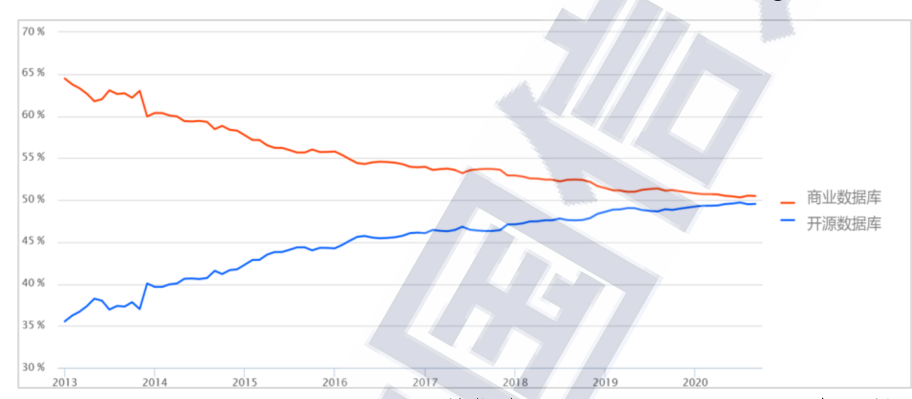
全球基础软件领域，开源占据主要市场份额。基础软件主要包括操作系统，数据库和中间件，操作系统可以细分为 PC 操作系统、手机操作系统、物联网操作系统、超级电脑操作系统等，根据 Linux 年度报告，在操作系统领域，Linux 分别占据 100%的超级计算机市场和 82%的智能手机市场，桌面操作系统市场排名第二；数据库可以分为关系型数据库与非关系性数据库，非关系型性数据库又可以细分为文档型数据库、图数据库、时序数据库、K-V 存储数据库等，根据 DB-Engines 数据显示，截至 2020 年 9 月全球开源数据库 182 个，已超过商业数据库 176 个；中间件可以按照功能分为消息中间件、事务中间件与远程过程调用（RPC）中间件，根据 enlyft 数据显示，Apache Kafka 占据应用集成领域 16.5%市场份额，同类型竞品中排名第一，Seata、Dubbo 也分别在事务中间件与 RPC 领域占据领先地位。

表 1 数据库市场情况

	名称	领域内排名	全市场排名
关系型数据库（开源占比 39.5%）	MySQL	2	2
	PostgreSQL	4	4
	Sqlite	7	10
非关系型数据库	文档型数据库（开源占比 80%）		
	MongoDB	1	5
	Couchbase	3	20+
	图数据库（开源占比 68.4%）		
	Neo4j	1	20+

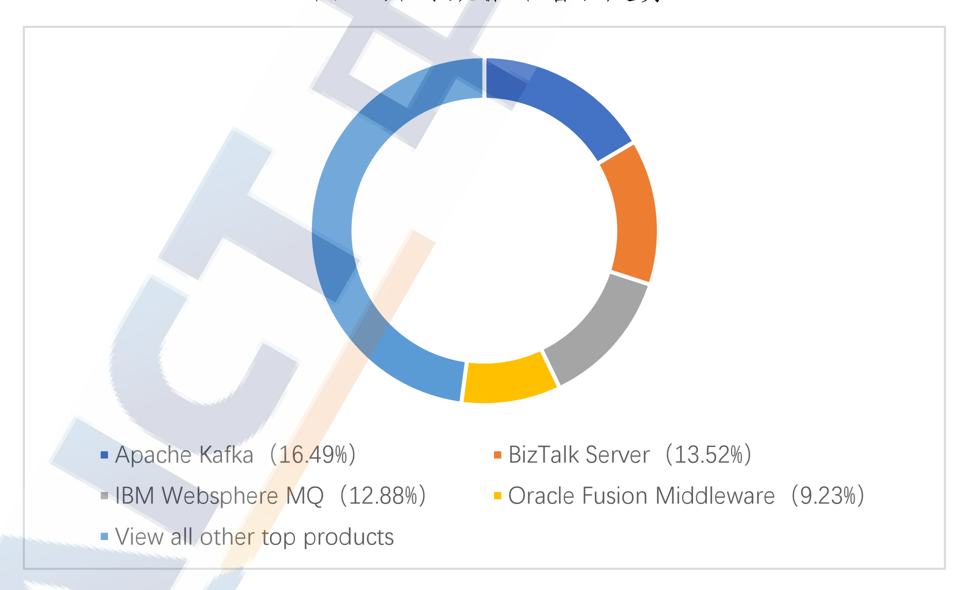
	OrientDB	3	20+
	时序数据库（开源占比 80.7%）		
	InfluxDB	1	20+
	Prometheus	3	20+
	K-V 存储数据库（开源占比 72.2%）		
	Redis	1	8
	memcached	4	20+

来源：DB-Engines ,2020 年 3 月



数据来源：DB-Engines，2020 年 9 月

图 7 开源数据库增长趋势



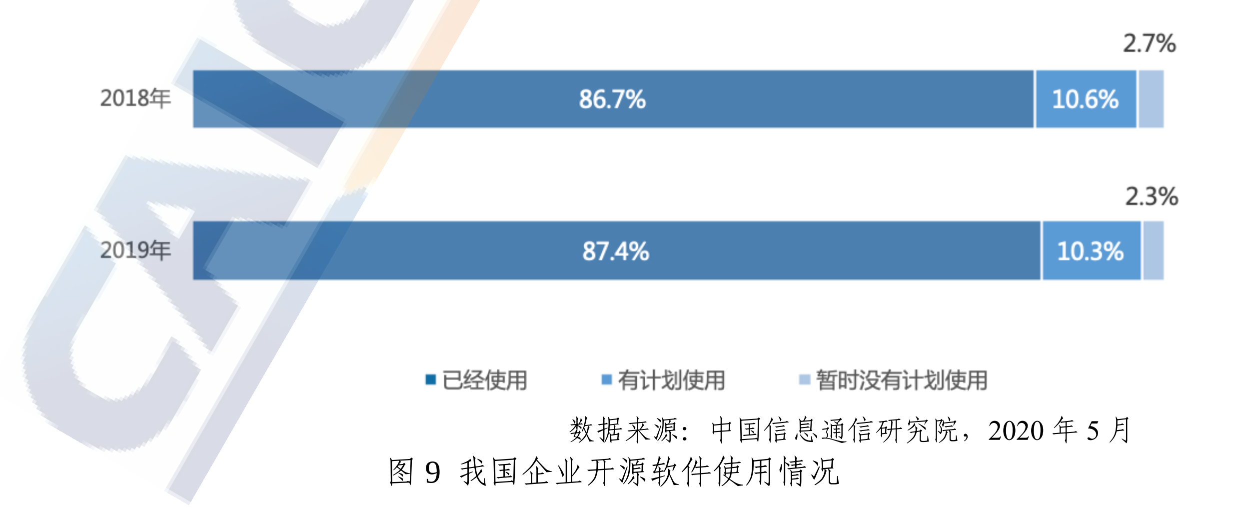
数据来源：enlyft，2020 年 8 月

图 8 Kafka 市场份额

全球新兴技术领域，开源成为主要技术路径。云计算领域涉及虚拟化、虚拟化管理等多个技术，以容器为代表的云原生技术路径是未

来云计算发展趋势，根据 CNCF 调查报告，2019 年 84％的公司在生产中使用容器，其中 78%的用户使用 Kubernetes 进行容器集群管理；大数据领域，大数据采集、大数据预处理、大数据存储及管理、大数据分析及挖掘、大数据展现和应用等关键技术，Hadoop 是大数据存储与管理的主要技术，根据 QYResearch 调查显示，到 2025 年全球 Hadoop 市场预计将达到 6708 亿美元，2017-2025 年年均增长 65.6%，亚马逊 EMR、谷歌 Dataproc、阿里云 E-MapReduce 和 AzureHDInsight 均选择基于 Hadoop 构建；人工智能领域涉及机器学习、知识图谱、自然语言处理、人机交互、计算机视觉、生物特征识别、AR/VR 等技术，其中机器学习框架是关键技术，TensorFlow 拥有 8 万多 Fork 数，位居同类型产品排名第一，Caffe 和 Keras 在学术界和工业界应用广泛，三者稳居深度学习库前三名。

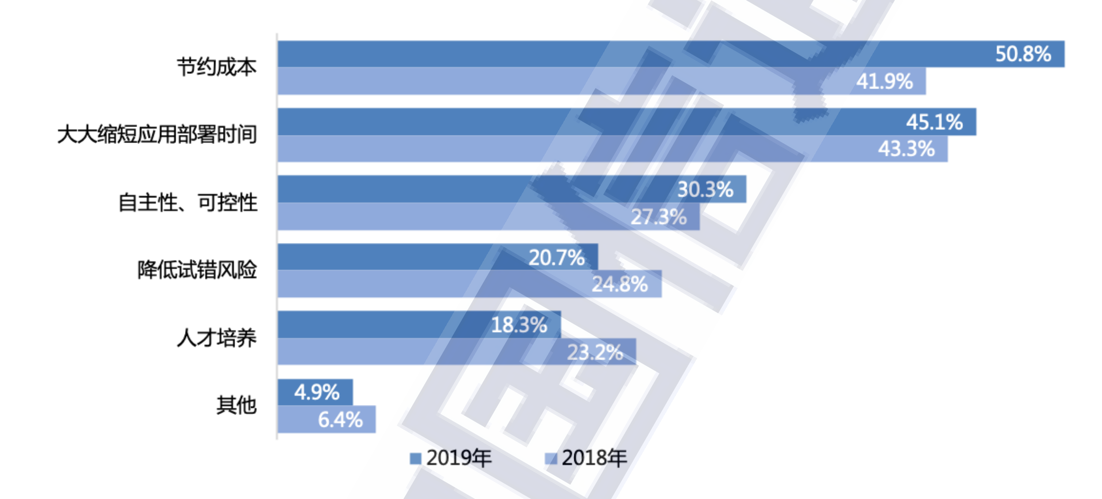
我国开源软件应用比例略有提升。根据信通院调查显示，2019 年我国企业已经使用开源技术的企业占比为 87.4%，比去年增长 0.7%，暂未计划使用开源技术的企业占比为 2.3%，比去年降低 0.4%，我国企业对开源技术的接受程度较高，使用开源技术已成主流。



数据来源：中国信息通信研究院，2020 年 5 月

图 9 我国企业开源软件使用情况

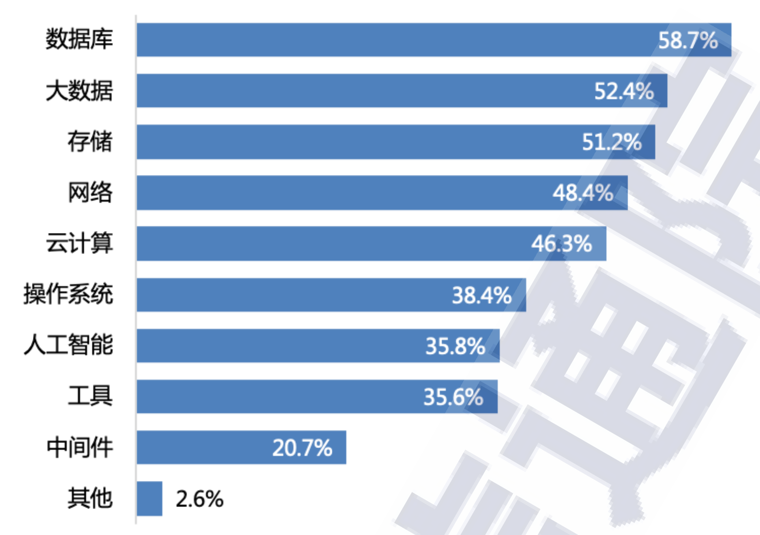
节约成本，大大缩短应用部署时间，成为我国企业选择使用开源技术最主要的原因。有 50.8%的开源用户企业认为使用开源技术可以节约成本，比去年增长 8.9%，认为使用开源技术可以大大缩短应用部署时间的企业占比为 45.1%，另外自主性、可控性（30.3%）和降低试错风险（20.7%）也是企业认为使用开源技术的两个优点。



数据来源：中国信息通信研究院，2020 年 5 月

图 10 企业选择开源软件原因

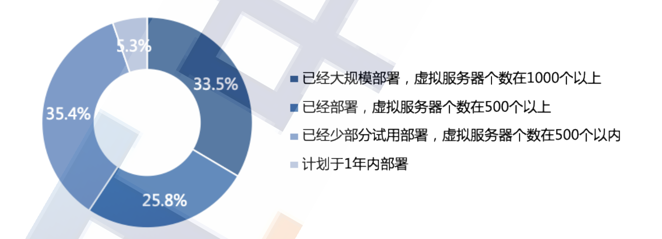
我国超半数企业使用开源软件应用于数据库方向。企业在数据库方面对开源软件的使用比例最高，占比为 58.7%，其次企业对大数据和存储的开源软件使用占比也均超过五成，分别为 52.4%和 51.2%，另外有 48.4%的企业在网络方面使用开源软件，有 46.3%的企业选择在云计算方面使用开源软件。



数据来源：中国信息通信研究院，2020 年 5 月

图 11 企业开源软件应用领域

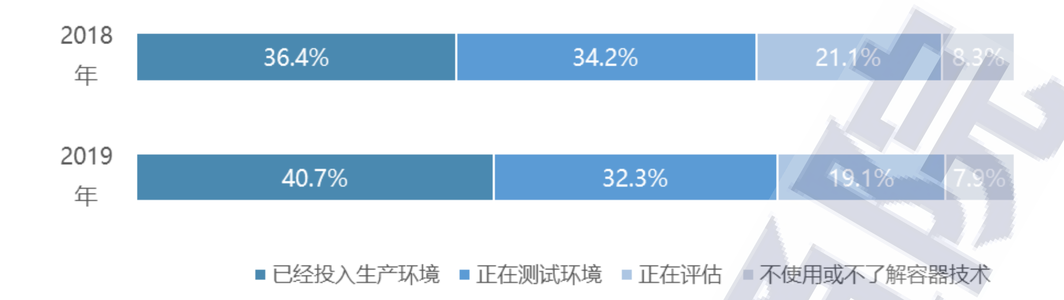
我国云计算领域已普遍应用云计算开源技术。据中国信通院调查，云计算开源解决方案部署虚拟服务器的个数在 500 以内的企业占比最高，达到 33.5%，虚拟服务器个数在 500 个以上的企业占比 25.8%，还有 35.4%的企业已少部分试用部署虚拟服务器。



数据来源：中国信息通信研究院，2020 年 5 月

图 12 我国企业云计算开源技术应用部署规模

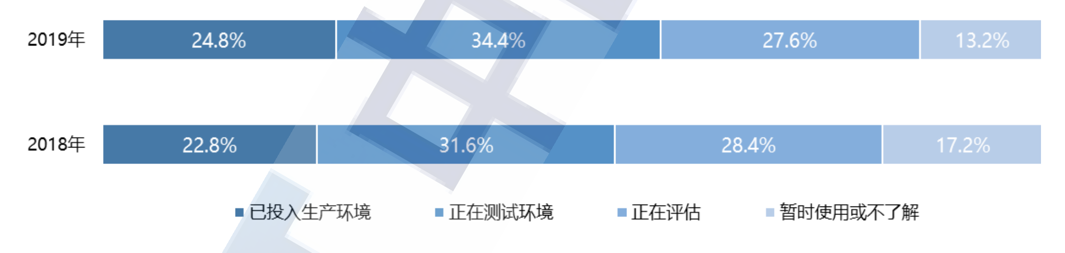
我国超过七成的企业已经应用开源容器技术。据调查，40.7%的企业已经使用了容器技术，相比 2018 年提高了 4.3%；其次，正在测试容器技术应用环境的企业占比达到 32.3%，比去年减少 1.9 个百分点。此外，还有 19.1%的企业正在评估容器技术。



数据来源：中国信息通信研究院，2020 年 5 月

图 13 容器技术应用情况

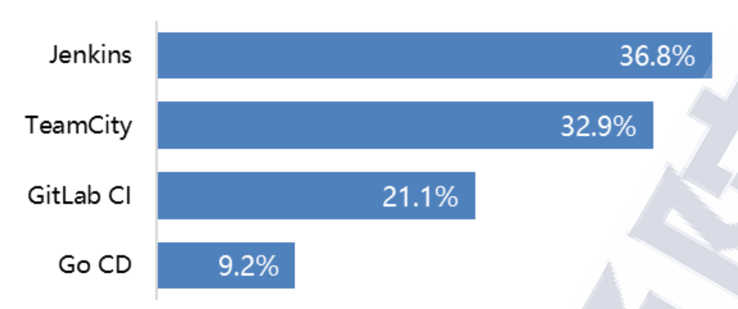
微服务领域以开源技术路径为主，我国超过六成企业已经应用或正在测试微服务框架。在对企业微服务框架使用情况的调查中发现，24.8%的企业已经应用微服务框架，相比 2018 年提高 2.0%；其次，正在测试环境的企业占比达到 34.4%，与去年相比提高 2.8%；此外，还有 27.6%的企业正在评估微服务框架。



数据来源：中国信息通信研究院，2020 年 5 月

图 14 企业微服务框架应用情况

Jenkins 是目前我国企业使用最广泛的开源集成工具。调查发现，在诸多开源集成工具中，Jenkins 的使用比例最高，达到 36.8%；其次，分别有 32.9%和 21.1%的企业表示已经应用 TeamCity 和 GitLab CI。此外，使用 Go CD 的企业占比为 9.2%。



数据来源：中国信息通信研究院，2020 年 5 月

图 15 企业使用开源集成工具情况

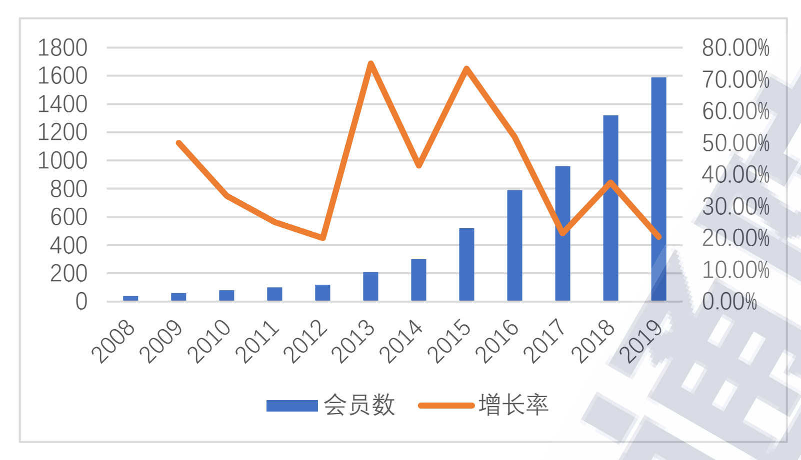
（三）开源企业数量保持稳定增长，我国企业呈现主动开源趋势

全球参与开源生态的企业数量激增。全球企业一方面积极参与开源代码贡献，开源代码托管是开源协作的必要条件，截至 2019 年 12 月 GitHub 参与的企业数接近 300 万；另一方面积极跟进开源组织，开源基金会是开源运营的一种模式，目前 Linux 基金会企业会员数超过 1500，是 5 年前会员数的 5 倍。



数据来源：GitHub，2020 年 7 月

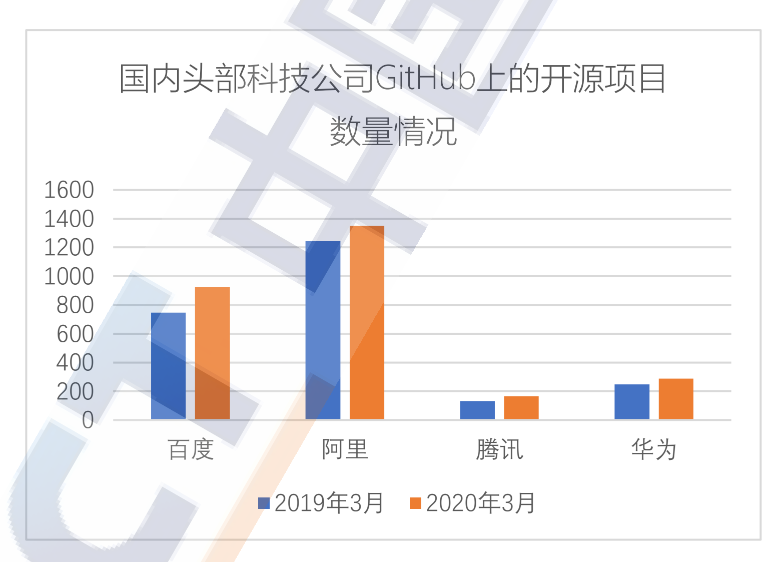
图 16 Github 近三年企业数量增长趋势



数据来源：GitHub，2020 年 7 月

图 17 Linux 基金会近十年会员数量增长趋势

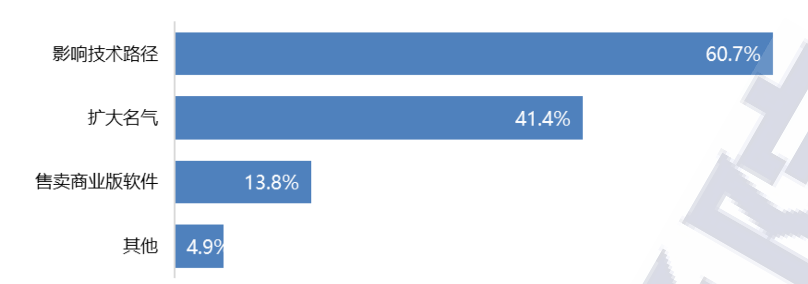
我国企业近年开源热度提升。近两年来，我国头部科技公司贡献大量开源项目，百度、阿里、腾讯和华为等企业开源数量连年增长。



数据来源：公开数据整理，2020 年 7 月

图 18 我国头部科技公司近两年 GitHub 开源项目数

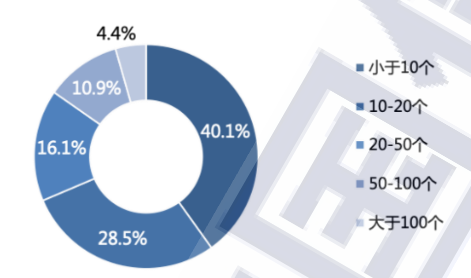
技术共建是我国企业参与开源的主要动机。根据信通院调查，60.7%的企业希望通过建设开源生态的方式影响共建技术，实现产品的完善与提升，其次，有 41.4%的企业希望能借助开源项目扩大企业名气。



数据来源：中国信息通信研究院，2020 年 5 月

图 19 企业积极开源的动机

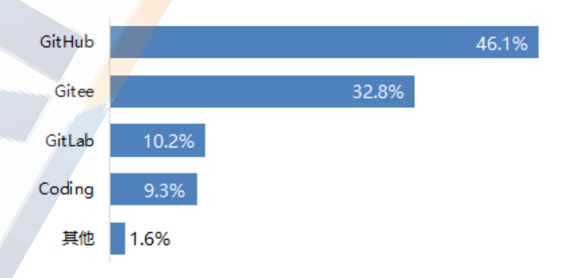
大范围发起开源的企业仍占少数。信通院调查发现，我国自发开源企业中，开源项目数量小于 10 个的企业占比为 40.1%，仅有 4.4%的企业开源项目数量超过 100 个。



数据来源：中国信息通信研究院，2020 年 5 月

图 20 自发开源企业的开源项目规模

GitHub 成为我国自发开源企业首选的开源代码托管平台。对开源自发企业调查发现，企业开源项目时最多考虑的代码托管平台是美国公司运营的 GitHub，比例高达 46.1%，其次选择的代码托管平台是中国公司运营的 Gitee，占比为 32.8%，另外还会考虑的开源代码托管平台是 GitLab（美国公司运营）和 Coding（中国公司运营）。

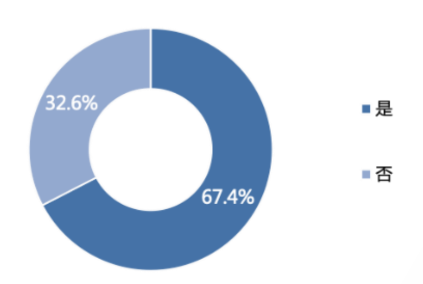


数据来源：中国信息通信研究院，2020 年 5 月

图 21 企业选择开源代码托管平台情况

超六成开源服务企业提供闭源软件。调查的开源服务企业中，有

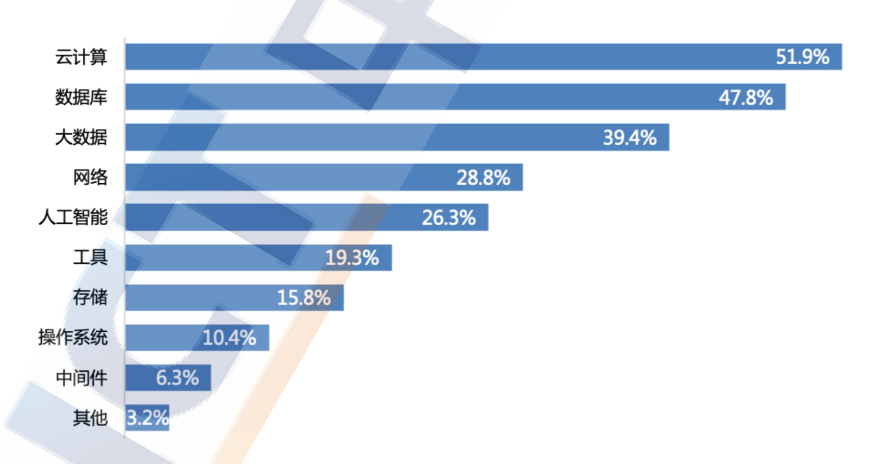
67.4%的企业拥有基于开源软件的闭源软件，说明开源服务企业提供开源服务时大多通过售卖封装好的闭源软件创造商业价值。



数据来源：中国信息通信研究院，2020 年 5 月

图 22 开源服务企业拥有闭源软件情况调查

云计算和数据库是开源服务企业的两大热门领域。调查显示，2019 年中国开源服务企业中 51.9%是基于云计算领域的开源软件进行二次开发提供开源服务，有 47.8%的产品是基于数据库领域的开源软件进行二次开发，此外网络（28.8%）和人工智能（26.3%）类开源软件也是开源服务企业进行二次开发主要选择的两个领域。



数据来源：中国信息通信研究院，2020 年 5 月

图 23 企业选择开源软件进行二次开发情况

（四）开源基金会成为开源运营重要角色

目前主流的开源基金（Linux 基金会、Apache 基金会等）是在美国国税局注册的 501(c)(3)或 501(c)(6)非盈利机构，近年来开源基金会

会员数及托管项目数不断扩充，我国企业积极参与国际开源基金会。

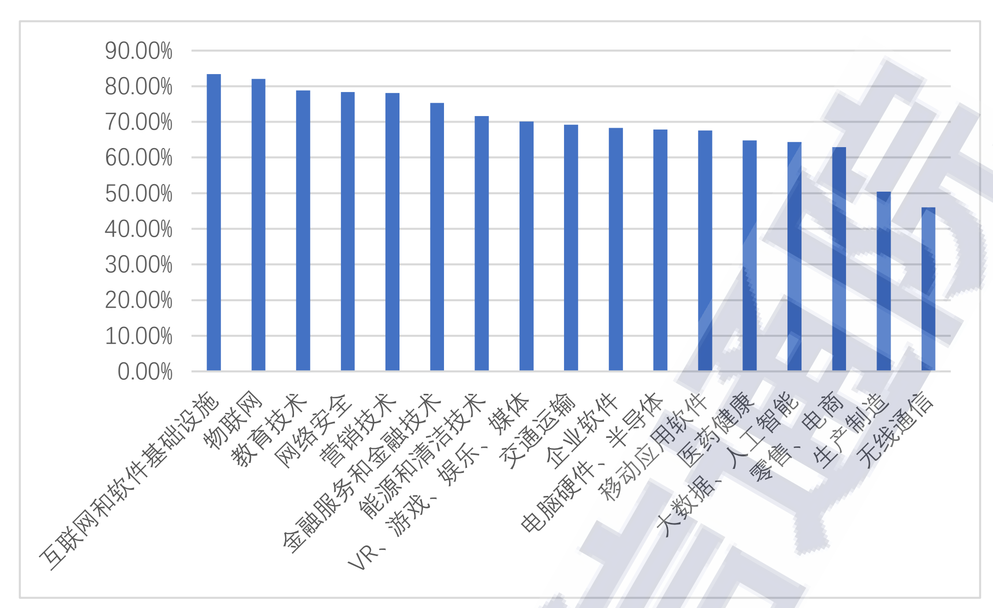
表 2 开源基金会会员及项目数量

开源基金会	会员数	托管项目数	中国会员数	中国项目数
Linux基金会（不包括子基金会）	607	100	28	15
Apache基金会	55	350	4	11
OpenStack基金会	140	56	9	-

来源：公开资料整理,2020年4月

（五）各行业开源生态已经形成，我国行业积极拥抱开源

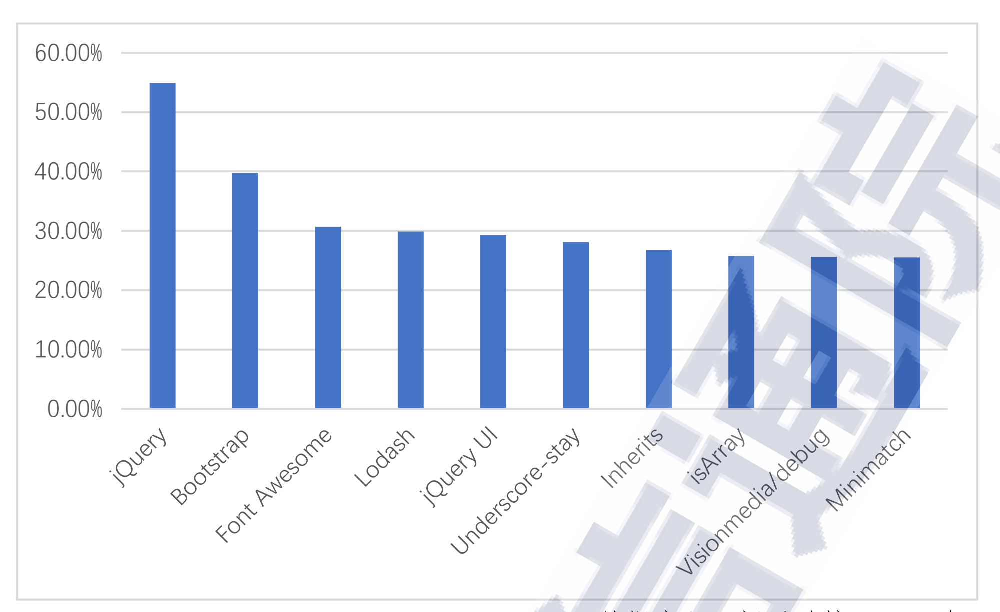
全球各行业开源应用均占据较高比例。根据新思科技发布的《2020开源安全与风险分析报告》调查显示，在可扫描的代码范围内，在互联网和软件基础设施行业以及物联网行业的代码库中分别有83.4%和82.1%是开放源代码；其次，在教育技术、网络安全、营销技术领域开源代码分别占比78.8%，78.4%和78.1%；金融服务和技术（75.3%）、能源和清洁技术（71.6%）、以及娱乐媒体行业（70.1%）也都是开源代码应用的热门领域。



数据来源：新思科技，2020 年 5 月

图 24 开源代码在不同行业代码库中的数量

根据新思科技发布的《2020开源安全与风险分析报告》显示，对全球1200多个代码库进行扫描统计出使用频率最高的前10名开源组件，jQuery是使用最多的开源组件，该组件是使用MIT许可证的开源软件，涵盖54.9%的扫描代码库和几乎所有的行业。其次是前端web框架开源组件Bootstrap，使用比例达到39.7%；第三名是一个基于CSS和LESS的开源字体和图标工具包组件Font Awesome，使用比例为30.7%；第四名是Lodash，它为常见编程任务提供实用函数的JavaScript库，使用比例为29.9%。其他6个开源组件和使用比例分别为jQuery UI，29.3%；Underscore，28.1%；Inherits，26.8%；isArray，25.8%；Visionmedia/debug，25.6%；Minimatch，25.5%。

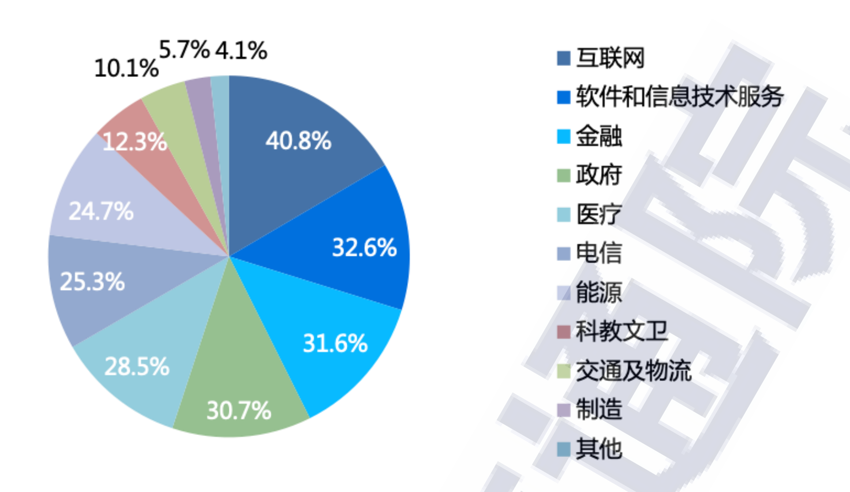


数据来源：新思科技，2020 年 5 月

图 25 热门开源组件及使用比例

全球传统行业积极跟进开源组织，并形成行业特色开源社区。 2019 年 Github 企业账号超过 300 万，AT&T、摩根大通、西门子等行业用户积极参与开源贡献; Linux 基金会会员同样覆盖重点行业用户，包括通用、NTT、富士通、中国移动、民生银行等。**重点行业及领域逐步形成特定开源社区，** 对于电信行业，Linux 合并的六个项目（ONAP、OPNFV、OpenDaylight、FD.io、PDNA 和 SNAS）成立 LFN 工作组，白金会员中覆盖全球 60％运营商；金融行业，2016 年成立金融行业开源社区（FINOS），2020 年成为 Linux 基金会的子基金会；边缘计算领域，Linux 基金会在 2019 年成立 LF EDGE 基金会，旨在建立独立于硬件、芯片的一个开放的、可互操作的边缘计算框架。

我国互联网、金融、软件和信息技术服务行业是开源服务企业主要的服务对象。 开源服务企业对互联网服务的占比最高，为 40.8%，其次是服务软件和信息技术行业，达到 32.6%，金融业也是开源服务企业的重要服务对象，服务占比达 31.6%。

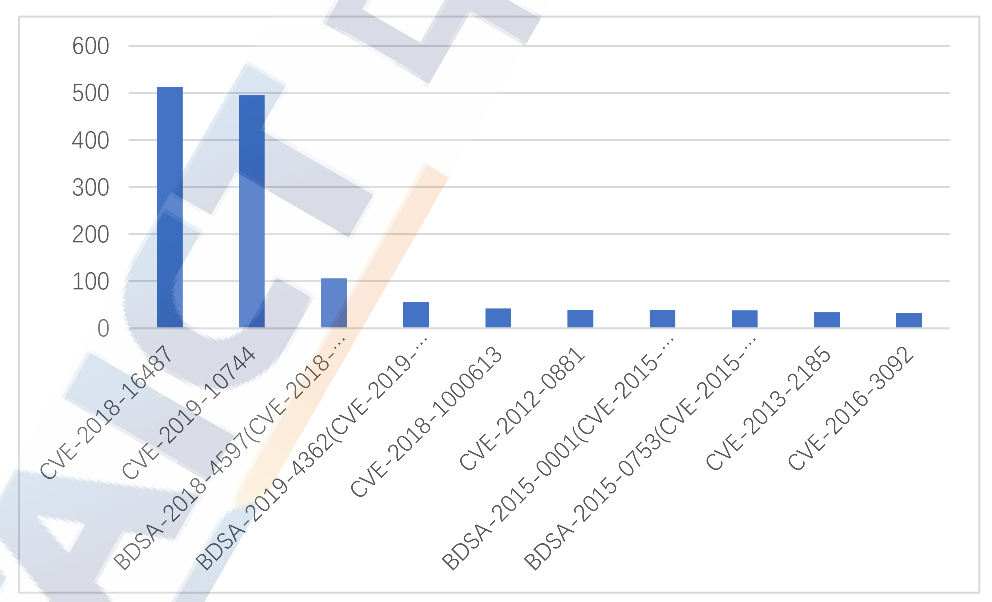


数据来源：中国信息通信研究院，2020 年 5 月

图 26 开源服务企业的服务对象分布情况

（六）开源风险问题凸显，成为开源应用屏障

存在漏洞的开源软件占比较高。根据 BD《2020 开源安全与风险分析报告》显示，75%的代码库至少含有一个漏洞，49%的已审核代码库包含高风险漏洞，发现最多的高危漏洞为 CVE-2018-16487，在 513 个代码仓库中发现此漏洞（高风险 Lodash 原型污染漏洞）。

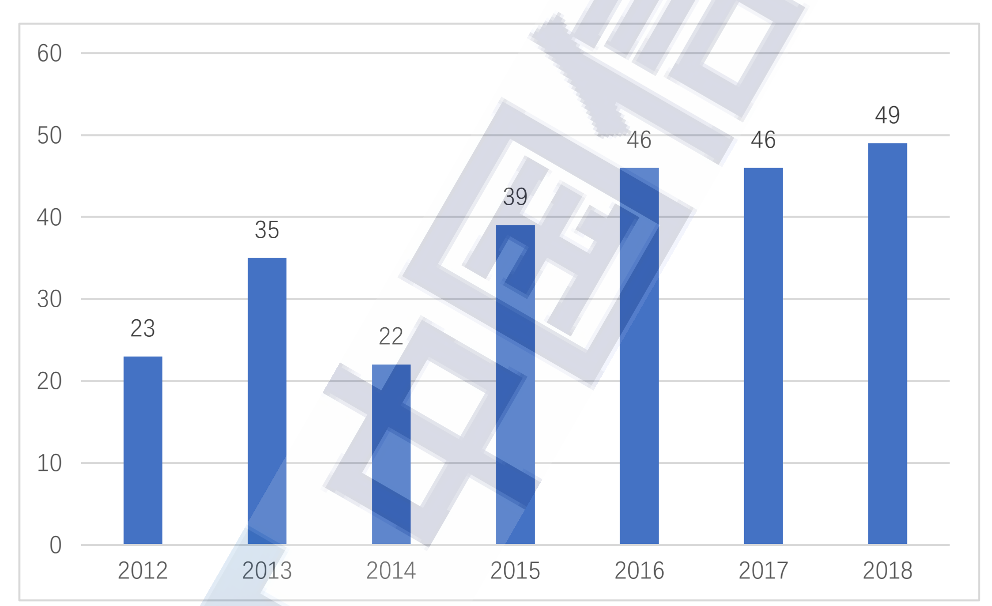


数据来源：新思科技，2020 年 5 月

图 27 风险漏洞占比

开源软件知识产权问题逐渐引起关注。根据 BD《2020 开源安全与风险分析报告》统计，67%的开源组件存在许可证冲突的情况，最

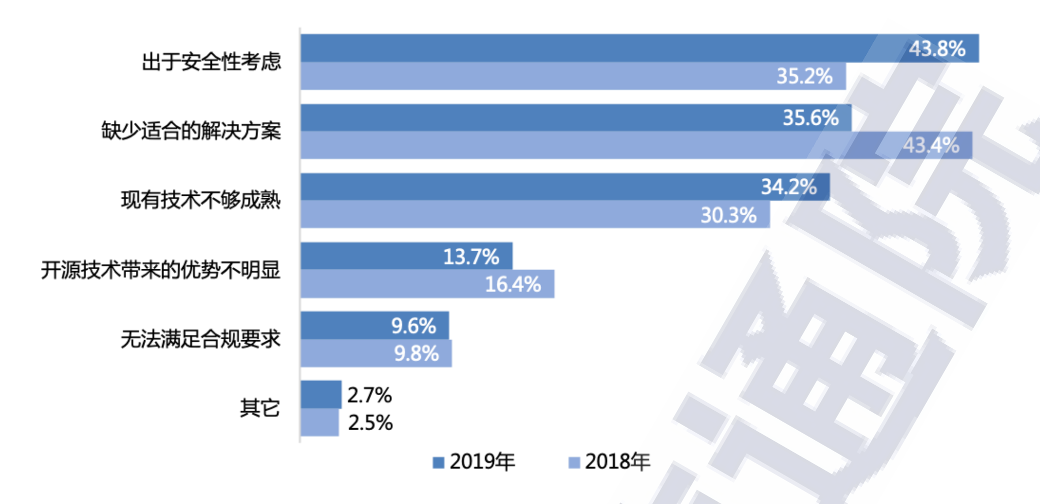
常见的情况是与 GPL 许可证存在兼容性的问题，GPL 是最常见的许可证之一，因此使用 GPL 许可证的开源项目数量较多，发生许可证兼容性问题的比例也是最多。根据美国专利组织 Unified Patents 公布的一项研究结果表明，2012 年到 2018 年底在美国地区法院共产生了约 260 个开源项目/平台的专利诉讼案例。中国 2019 年也出现了第一例涉及 GPL 开源许可证的诉讼案例，这起案件是因侵犯计算机软件著作权所产生的纠纷案。



数据来源：Unified Patents，2019 年 11 月

图 28 美国 2012-2018 年开源项目/平台的专利诉讼案例数量

出于安全性考虑成为我国企业尚未应用开源技术的最主要原因。2019 年，出于安全性考虑而未使用开源技术的企业占比最高，达到 43.8%，比去年增加 8.6%，而 2018 年占比最高的是缺少适合的解决方案，在 2019 年占比为 35.6%，比 2018 年降低 7.8%，降至第二位，反映出企业对于开源治理的诉求更加迫切。



数据来源：中国信息通信研究院，2020 年 5 月

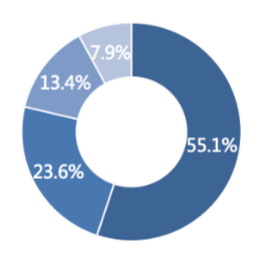
图 29 我国企业未使用开源软件的原因

（七）全球开源治理理念兴起，我国初步形成开源治理模式

开源治理是针对开源引入过程、自发开源过程、开源社区维护等方面的一套流程体系，是推动开源生态良性发展的有效手段。

全球部分企业正在规划开源办公室。根据 Linux 基金会开源办公室调查报告显示，在 2,700 名研究参与者中，超过一半（52%）拥有正式或非正式开源项目办公室，或者他们的公司计划创建一个计划。

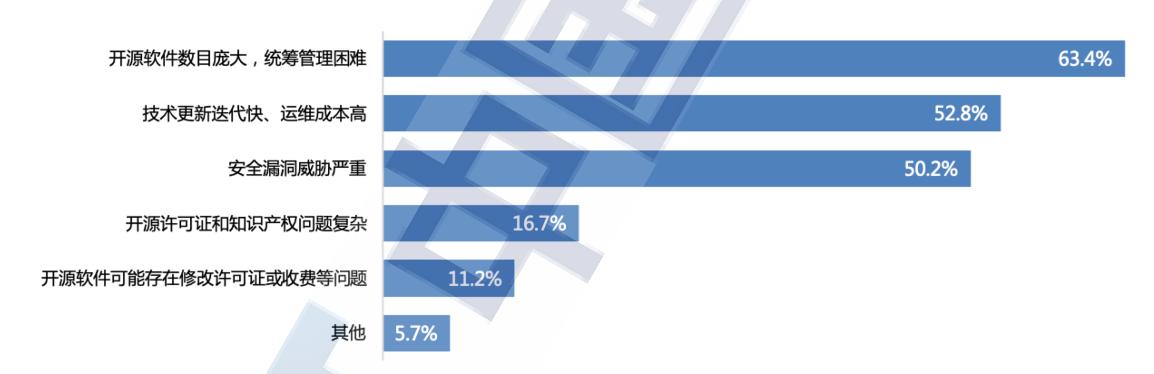
我国企业逐步关注统一开源治理。开源软件数目庞大，统筹管理困难成为企业最关注的开源软件引入风险点，23.6%的受访企业有统一管理流程和管理团队，13.4%的企业有白名单或黑名单机制，55.1%的企业目前对引入的开源项目没有统一管理，主要由开发运维团队分散管理。



数据来源：中国信息通信研究院，2020 年 5 月

图 30 企业开源治理情况调查

开源软件数量庞大是开源治理的主要难点。对开源用户企业调查发现，开源软件数量庞大，统筹管理困难是企业关注的开源软件引入的最主要风险，占比达到 63.4%，技术更新迭代快、运维成本高（52.8%）和安全漏洞威胁严重（50.2%）也是企业认为引入开源软件会遇到的主要风险。



数据来源：中国信息通信研究院，2020 年 5 月

图 31 企业认为开源软件引入产生的风险情况

（八）开源配套政策正在完善，我国政策引导开源社区构建

全球通过政府采购市场调动开源生态。美国联邦政府于2016年推出联邦源代码政策，规定美国政府各部门每年采购的软件中20%的代码需开源；**韩国**政府拟在2026年前让所有公共机构和地方政府采用基于Linux的OpenOS系统，同时使用OpenOS系统将有效减少采购商业操作系统以及操作系统技术支持方面的开支；**英国**政府在2019年发布

的最新版《**数字服务标准**》第12条要求政府部门公开所有新的代码，并选择合适的许可证开源。

政府部门引导产业关注开源风险问题。欧盟推出“IDABC”计划解决开源许可证的风险问题，欧盟通过制定欧盟公共许可证EUPL促进各成员国共享和重新利用由公共机构和行政机构开发或为其开发的软件；**澳大利亚**政府单独发布《澳大利亚和政府开源软件许可风险框架》，概述开源许可风险的重要性，提供识别和管理开源软件许可证相关的风险方法；**英国**政府发布《开放代码的安全注意事项指南》；**美国**联邦金融机构审查委员会发布《开源软件风险管理指引》。

政府相关部门加大开源方面投入。美国科研院所引领开源生态，美国科研院所从开源项目的使用者向开源项目的贡献者转变，截至 2020 年 4 月，美国 NASA 在 Github 上托管 261 个开源项目，同时 NASA 建立了自己的开源代码托管平台，托管 560 个开源项目（源码、开放数据、开放 API 等），阿贡国家实验室在 Github 上共托管 160 个开源项目，洛斯阿拉莫斯国家实验室在 Github 上共托管 38 个开源项目，这些开源项目在各自领域具有重要价值，并逐步形成自己的开源生态。**欧洲**核子研究机构（CERN）在开放数据、开源硬件有一定积累，在 GitHub 有 6 个开放数据的项目。

我国政策关注开源社区发展。一方面国家层面鼓励产业加大开源投入，2016 年发改委发布“十三五”国家信息化规划的通知（国发〔2016〕73 号），推动龙头企业和科研机构成立开源技术研发团队，支持开源社区创新发展，鼓励我国企业积极加入国际重大核心技术的

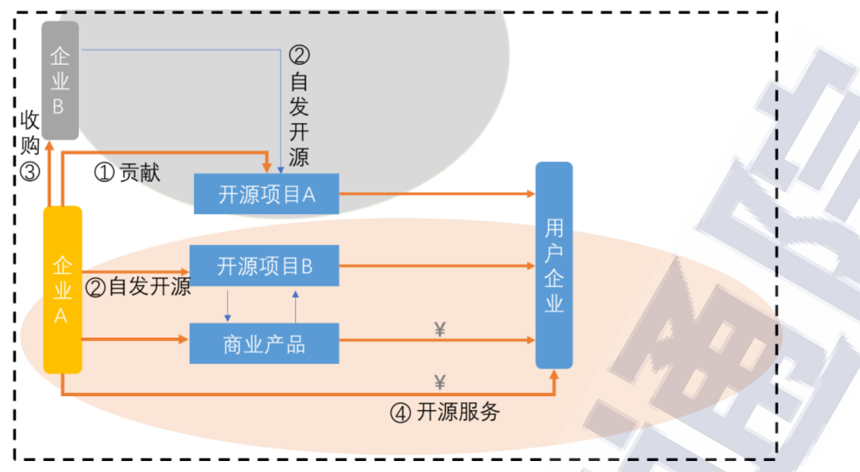
开源组织；2020 年 4 月国家发展改革委、中央网信办研究制定了《关于推进「上云用数赋智」行动培育新经济发展实施方案》，该方案加大对共性开发平台、开源社区、共性解决方案、基础软硬件支持力度，鼓励相关代码、标准、平台开源发展。另一方面，地方政府关注开源社区及开源软件的创新使用，2019 年，湖南省发布《湖南省大数据产业发展三年行动计划（2019-2021 年）》，支持建立大数据相关开源社区等公共技术创新平台，鼓励开发者、企业、研究机构积极参与大数据开源项目，增强在开源社区的影响力，提升创新能力；2018 年，山东省发布《数字山东发展规划（2018-2022 年）》，支持基于开源软件的消化吸收再创新。

三、开源成为企业商业布局的重要手段

开源贡献者与开源服务者结合自身经营模式与开源进行有效结合，实现商业转换。

（一）全球开源商业模式多样化发展

企业可通过主动开源进行商业布局，一是积极跟进相关领域顶级开源项目，深度参与开源贡献，影响开源技术路线；二是建立自发开源生态，将有可能影响市场格局的项目开源，同时培育潜在用户，推动形成事实标准；三是收购特定领域开源企业，与自身商业产品配合，扩大用户市场；四是结合开源项目提供开源服务，通过开源服务实现商业转化。



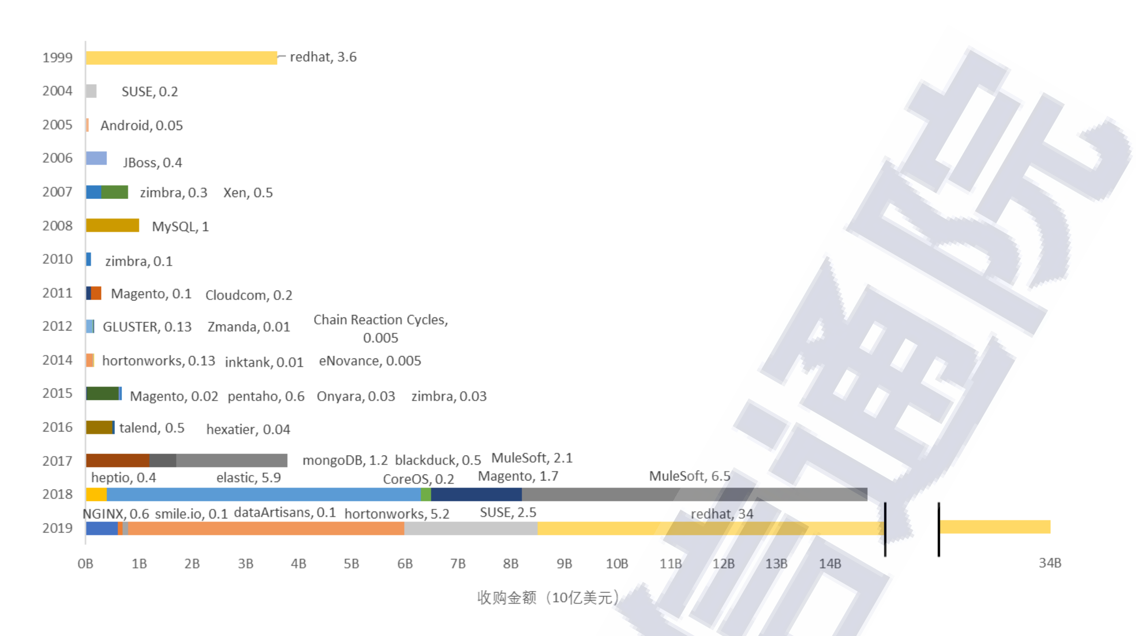
数据来源：中国信息通信研究院，2020 年 8 月

图 32 开源商业布局的四种方式

（二）全球开源企业已启动收购模式，进一步扩大用户群体

全球开源投资步伐逐渐加快。ANDREESSEN HOROWITZ是一家在硅谷成立的风投公司，关注科技领域，共投资了29家开源公司总计702.75亿美元；IBM通过对开源的持续投资获得收益，除2018年以340亿美元市值收购红帽公司外，IBM在过去五年中投入开源近10亿美元；微软2018年以75亿美元收购GitHub；2020年SUSE收购业界应用最为广泛的Kubernetes 管理平台建设方Rancher。





数据来源： Pitchbook，2020 年 4 月

图 33 开源投资情况

全球开源企业积极布局开源，率先在基础软件领域发力，带动整体商业布局。顶级科技公司成为开源的重要贡献者，微软、谷歌、红帽、英特尔等顶级科技公司的员工是开源项目的重要贡献者。根据 Github 统计，微软有 7700 名员工参与开源投入，谷歌有 5500 人参与开源投入。谷歌开源移动操作系统 Android，截止 2019 年 8 月，在全球移动操作系统市场中占有率高达 75.44%；开源 PC 操作系统 ChromeOS，在美国有一定市场地位，其市场占有率高达 4.82%。微软开源跨平台编译器 VScode，自 2016 年起连续占据 GitHub 开源项目 TOP10，2018-2019 稳居榜首，由它部署的 Azure 在 2018 年市场收益达到 48.6 亿美元，占据云计算市场 17%份额；Facebook 开源对象关系数据库服务器 PostgreSQL，2020 年 3 月，DB-Engines 数据库流行度排行榜第四名。

基于开源逐步形成稳定的商业模式。开源社区版本多以公开形式发布源代码，围绕社区版开源项目，很多企业已经形成服务为主的商

业模式。**一是开源服务订阅收费，**这种模式是向企业客户提供基于上游开源社区软件代码打造的企业级开源软件产品，把开源社区的项目产品化，使普通企业客户更容易消费开源创新技术，例如红帽把按年度的收费模式叫做“订阅模式”，除了免费享受这些支持以外，用户无需再次购买产品的升级，根据用户的需要可随时进行更新；**二是企业发行版收费，**随着开源协议授权条款的松绑，软件公司可基于社区版的基础功能，提供自己研发的企业发行版本，这些企业发行版一般会收取费用，并且是闭源的，此模式的代表公司是 Apache Hadoop 生态圈知名度最高的 Cloudera 公司，围绕 Apache Hadoop 提供企业级解决方案，主要的客户集中在中大型企业客户；**三是云服务收费，**随着云计算逐渐被市场接受，整个云端应用能力大幅成长，这也促成了新的开源服务商业模式，即采用付费直接使用云端服务的商业模式，企业客户直接付费使用构架在云端的开源软件，不用自己搭建软件使用环境，使得技术能力不强的中小型企业也能以较低成本享受开源技术，也因相关云端技术的成熟，云计算订阅的收费模式开始大行其道，亚马逊等公司就是这类新创开源软件公司的代表。

（三）我国开源企业已初步构建形成有影响力的开源项目

我国积极跟进国际开源生态。参与国际顶级开源社区反馈，实现技术输出，共建技术路径，GitHub 国内贡献数 117 万，在全球占比 11.8%，Linux 项目中国在全球贡献度排名第三。

我国构建自发开源生态，开源项目影响力呈现持续扩大态势。我

国企业主动开源形成稳定自发开源模式，互联网企业紧跟产业数字化机遇，借助流量优势开源项目，截至 2020 年 9 月，阿里开源 2172 个项目，腾讯开源 150 个项目，总体同比保持 15%的增长率，设备厂商勇于打破原有商业模式，积极拥抱开源，截至 2020 年 9 月，华为开源 161 个项目，我国自发开源项目中不乏国际影响力开源项目，其中 Dubbo、RocektMQ、CarbonData 等均已成为 Apache 顶级开源项目。移动互联网企业也在积极开源，小米 MACE（移动端 AI 框架）和 Pegasus（分布式 KV 存储）和 Kaldi 均已开源。

头部科技公司在代码托管平台上的开源项目数呈明显增长趋势，根据 2019 年《中国互联网公司开源项目调查报告》[1]显示，阿里、腾讯、百度、华为等头部互联网企业在 Github 上贡献的数量超过 3000，集中在前端开发、人工智能、数据库、微服务、中间件等领域。

表 3 我国企业在 Github 代码贡献情况

国内排名	全球排名	项目名称	公司
前端开发			
2	28	ant-design/ant-design	阿里巴巴
3	37	ElemeFE/element	阿里巴巴
5	90	NervJS/taro	京东
7	107	vuejs/vue-cli	——
10	141	ant-design/ant-design-pro	阿里巴巴
11	169	apache/incubator-echarts	百度
12	193	vuejs/vue	——
14	209	youzan/vant	有赞
15	237	nestjs/nest	——
26	477	vuejs/vuepress	——
人工智能			
6	103	PaddlePaddle/Paddle	百度
18	297	ApolloAuto/apollo	百度
20	383	PaddlePaddle/models	百度

[1] http://www.199it.com/archives/856967.html

25	452	huaweicloud/ModelArts-Lab	华为
数据库			
8	128	pingcap/tidb	PingCAP
21	385	tikv/tikv	PingCAP
微服务			
16	270	apache/dubbo	阿里巴巴
19	362	alibaba/nacos	阿里巴巴
23	394	apache/skywalking	——
中间件			
22	389	seata/seata	阿里巴巴
24	426	apache/ shardingsphere	京东数科
其它			
1	2	996icu/996.ICU	——
4	83	selfteaching/selfteaching-python-camp	——
9	137	OpenAPITools/openapi-generator	——
13	207	Advanced-Frontend/Daily-Interview-Question	——
17	296	xitu/gold-miner	掘金

数据来源：X- lab 开放实验室

头部科技公司在基础软件领域的开源项目呈增长趋势，开源将成为未来新技术发展的重要抓手。华为开源服务器操作系统 EulerOS，跨平台的操作系统 HarmonyOS，单机版数据库 GaussDB OLTP，全场景 AI 计算框架 MindSpore；腾讯开源轻量级物联网实时操作系统 TencentOS tiny，万亿级分布式消息中间件 TubeMQ，企业级分布式 HTAP 数据库管理系统 TBase；阿里开源实时计算平台 Blink，云服务器架构“方升”，关系数据库 OceanBase。

战略投资实现开源资源整合。腾讯投资代码托管平台 Coding、百度投资代码托管平台开源中国、阿里巴巴以 9000 万欧元收购了 Data Artisans（开源项目 Flink 发起公司），国内科技公司积极投资开源基础设施，为构建自身生态做好铺垫。

云计算推动我国开源服务发展。我国阿里云、中兴、腾讯云等众多企业基于 Kubernetes、Docker 等开源软件构建闭源商业产品，形成稳定的发行版收费模式；阿里云服务为用户提供多种云计算服务，这些服务部分基于开源软件提供，如云数据库类是基于 MySQL，Redis，MongoDB 等热门开源数据库提供云服务。

四、全球开源基金会运营模式成熟，我国率先探索联盟运营机制

（一）良好的开源社区是形成开源代码的前提条件

全球已形成大批以技术为中心的开源社区。开源社区一般依托开源项目自然形成，是开源项目不断发展的重要组织，开源社区数量基本与开源项目数量等同。开源社区聚集一批对开源项目感兴趣的人，主要进行代码协作、开源讨论、社区决策等工作，全球开源项目过亿，已经形成相对稳定的开源社区运转模式。根据参与者范围开源社区运转可分为以下两种模式，一种是**集市模式**，鼓励任何人都可以做出贡献，具有快速迭代特点，例如 Linux；一种是**大教堂模式**，由相对稳定的团队进行贡献，发布频率相对较低，例如 Apache OODT。根据决策机制，开源社区运转可分为以下两种模式，一种是**精英模式**，根据贡献程度形成决策结构，Apache 基金会开源项目所依托的开源社区均采用精英模式；一种是**独裁治理模式**，即项目的把控者是其创始人和资助者。

表 4 开源社区分类

典型开源社	Linux 社区	Apache OODT	Apache	Ubuntu 社区

区		社区	HTTPD 社区	
参与者	任何人	相对稳定的团队	任何人	相对稳定的团队
决策机制	创始人和资助者	根据贡献度形成决策机制	根据贡献度形成决策机制	创始人和资助者
开源模式	集市模式;独裁模式	大教堂模式;精英模式	精英模式;集市模式	独裁模式;大教堂模式

来源：公开资料整理,2020 年 4 月

我国以用户为中心的开源社区发展阶段与全球保持一致。不同行业对开源的需求往往是各不相同，为满足不同行业对开源的具体需求，行业开源社区应运而生。中国信通院联合浦发等多家金融机构成立“金融行业开源技术应用社区”，规范开源治理体系、讨论开源软件选型标准和建立开源软件共享平台，全球开源用户社区仍处于探索阶段，FINOS 基金会成立四年于 2020 年与 Linux 基金会合作，寻找用户社区发展新模式。

（二）开源基金会运营通过知识产权托管培育开源社区

开源基金会主要进行开源项目第三方知识产权托管，同时提供配套服务建立开源生态，一般对开源项目进行资金众筹和支持，提供相关法律支持，聘请专业人员进行管理，建立专业化人才培训机制，借助通用规则保证开源项目安全性。

开源基金会的战略布局由董事会决策。各基金会董事会形成方式不同，Linux基金会董事会（25人）主要由白金企业会员代表组成；Apache基金会董事会（9人）由700余个人会员根据贡献度选举产生；

OpenStack基金会（24人）主要由白金会员和黄金会员代表组成。董事会对基金会的战略规划、财务管理、市场及法务问题、分支机构设立具有决策权，通过投票表决方式决议。董事会不参与开源项目的日常技术管理，重量级的子基金会/项目拥有自己的董事会来进行自治。Linux董事会每个成员都有投票权，并且决策通过需多数成员投票同意；Apache董事会采用懒惰共识法，决策需要没有反对票的正面投票，当投反对票时，要明确提出替代方案，以及投反对票的详细解释。

技术管理委员会对开源项目进行技术指导。基金会整体技术管理委员会负责技术指导，Linux基金会建立技术咨询委员会，由Linux主要的贡献者组成，主要提供技术咨询，OpenStack基金会技术管理委员会由13名个人组织，负责技术管理和指导，参与决策项目的孵化和毕业，对各个开源项目无直接管理权；单个项目技术管理委员会直接管理开源项目，对于Apache基金会，每个项目都会形成技术管理委员会，项目发展路径和定位由项目管理委员会投票决定。

管理团队负责基金会日常事务，部分基金会聘请专职人员。Linux基金会建立专职经营团队，包括执行董事、项目经理、财务主管、基金会秘书等角色，负责市场营销、项目合规、培训、项目孵化等执行工作，高级职员一般每两年选举一次，且由董事会进行任命；Apache基金会具有专职执行总裁、财务总监、秘书等角色构成管理团队负责基金会管理与监督，财务以及市场活动采用外包形式，以减少成本与提升效率。

会员构成开源基金会交流平台。Linux基金会为企业会员模式，

目前白金会员15家，黄金会员15家，白银会员800余家，白金会员可最多任命20名董事会成员，新会员入会需董事会进行决议；Apache基金会为个人会员模式，会员都是以个人身份参与项目组织，专注于技术交流，新的个人会员由现有个人会员提名，然后根据该成员对基金会的贡献情况进行投票，企业仅以赞助的形式参与，获得网站展示标识以及会议发言机会；OpenStack基金会为企业会员模式，只容纳最多8家白金会员资格和24家黄金会员资格，白金与黄金会员可以各自选举8名董事会成员，董事会有权利进行新会员资格投票，终止或恢复企业会员资格。

开源基金会收入来源逐渐多样。目前主流的开源基金会都是非营利性组织，资金主要来源依赖于企业会费（企业捐赠）以及日常运营的收入（项目管理、活动、培训与认证）等；会员费作为开源基金会的主要收入来源，Linux基金会白金会员50万美元/年，黄金会员10万美元/年，白银会员5000-20000美元/年，Linux基金会年会员费收入超过1000万美元，总收入占比50%左右；Apache基金会资金主要来源于企业捐赠，捐赠等级分为白金12.5万美元/年，黄金5万美元/年，白银2.5万美元/年与青铜6千美元/年，年收入191万美元；项目管理费收入占比逐渐提升，Linux基金会对子基金会及重要项目收取项目管理费用，目前项目管理费用占linux基金会总项目收入的40%。

基础设施与人员投入作为基金会的主要开销。根据Apache基金会财报，支出费用从2018财年的142万美元增长至2023财年的220万美元，支出费用中基础设施占比最高，达到34%；Linux基金会的设施服务

费从2017年的423万美元增长到2018年的1856万美元，增幅达到338%，人员薪酬费用也从2017年的2254万美元增长到2018年2529万美元，增幅达到12.2%。

（三）我国逐步形成稳定的开源运营机制

开源运营最终目的是推广开源项目的认可度，建立开源生态，我国一方面推动开源基金会相关工作，另一方便借助联盟优势推动开源运营。

开源基金会实体机构已经形成。开放原子开源基金会于2020年6月正式在民政部注册成立，是非营利性独立法人机构，针对开源软件、开源硬件、开源芯片及开源内容等提供中立的知识产权托管，并提供资金，法律、财务等专业支持。理事会是开源基金会的立法机构，负责审议和修改基金会章程等；技术监督委员会是技术决策机构，负责开源基金会技术相关的决策；秘书处是开源基金会的执行机构，负责开源基金会日常运营事务等相关工作。目前基金会托管开源项目7个，主要捐赠单位包括阿里、百度、华为、浪潮、腾讯、360、招商银行等。

联盟开源运营机制持续推进。联盟社区开源运营机制不进行开源项目知识产权托管，主要进行技术治理和业务治理，通过行业社区推动开源项目建立自生态，中国信通院重点依托工业互联网联盟、云计算开源产业联盟、金融行业开源技术应用社区、人工智能产业发展联盟等行业及新技术领域产业资源，帮助企业运营开源项目，目前与腾讯蓝鲸、TARS等项目建立合作关系，主要通过会议宣传推广、产品

标准制定，上下游一致性评估、人才培养认证等方面工作，管理开源项目的社区，在人工智能等新技术领域创建开源开发者社区平台、开源咨询管理平台、构建人工智能大赛平台，促进开源项目的生态发展。

五、传统行业逐步拥抱开源生态，我国行业用户关注开源使用

（一）工业互联网布局开源看重产业数字化新机遇

在工业互联网领域，巨头企业更多看重的是把握工业互联网浪潮中产业数字化转型的新机遇，占领新兴产业的制高点和影响力。

全球工业互联网领域在物联网方向开源投入积极。目前，工业互联网积极布局开源项目，主要侧重 IoT 领域。龙头企业正在尝试基于通用开源软件建立工业互联网领域开源生态，西门子在 GitHub 上的自发开源项目为 38 个，涉及 IOT2000 设备硬件特性管理等项目。GE 的开源策略经历了三个主要阶段，一是依赖技术投资阶段，GE 与 EMC 联合向 CloudFoundry 架构供应商 Pivotal 进行投资，以实现对关键技术的掌控；二是自发开源阶段，自 2016 开源工业互联网平台 Predix，尝试建立类似 Android 生态；三是开放社区阶段就是通过开放的 API 接口建立生态。IoT 领域开源软件逐渐兴起并多由创业公司发起，且 KAA，Zetta 等开源软件背后均有商业化服务。工业互联网领域开源协同机制已经形成，集中在边缘计算及物联网领域，如 Eclipse IoT 工作组，LF EDGE 工作组等。

我国工业互联网领域市场应用旺盛，科技公司率先布局。我国工

业互联网领域对工业互联网 PaaS 平台、边缘计算框架、边缘云开源技术需求最为旺盛。在开源投入方面，科技公司率先布局开源生态，发力边缘计算平台和物联网操作系统领域，比如华为的 KubeEdge，百度 OpenEdge，阿里 AliOS Things，腾讯 tencentOS-tiny 等，高校在物联网数据库领域积极探索开源模式，由清华大学发起的 Apache IoTDB 已经成为 Apache 顶级项目；在产业协作方面，科技公司探索建立开发者社区，形成产业协作模式，如小米投入 1 亿元打造小米 AIoT 基金会、浪潮牵头成立中国开源工业 PaaS 协会。

（二）电信行业由用户侧及运营商推动开源，探索产品创新

电信领域技术壁垒高，研发投入高，电信基础设施和应用/服务的生命周期很长，对研发以及运维团队要求高。电信行业运营商和大型互联网公司积极拥抱开源，主要是为了摆脱设备厂商锁定，基于自身的业务，能够主动、高效且低成本的满足对设备的需求，同时也有部分新兴设备厂商探索开源，尝试打破市场垄断，但是大设备商供给侧市场稳定，开源动力不足。

全球电信行业在网络各个层面开源投入积极，生态多样。电信行业开源生态覆盖开源软件和硬件，其中开源软件发展尤为繁荣。从网络数据分析软件、编排管理策略软件等上层应用软件，到构建网络功能的 NFV 软件，再到虚拟化管理、网络控制、网络操作系统等基础软件，都有大量的开源项目，如 Acumos、Open-O、OPNFV、OpenStack、ONOS、OpenSwitch 等。底层硬件设计也有一些开源白盒项目，但相

对较少，例如由 Facebook 发起的 Open Compute Project 项目。



数据来源：根据公开资料整理，2020 年 6 月

图 34 电信行业开源项目

电信行业与互联网巨头均大力投入电信领域开源项目投入，自成生态，例如 AT&T 主导多个主要的开源项目，包括 ONAP、DANOS 等，Google 开源 Stratum，Facebook 推动成立 OCP（开放计算项目）。针对网络领域的开源产业协同机制已经建立，包括开源基金会、生态社区等形式，开源基金会主要包括 LFN（Linux 基金会）、OCP（开放计算项目）、ONF（开放网络基金会）等，基金会会员覆盖了全球超过 70%的电信产业链上的玩家，其项目覆盖基础设施/接入/承载/核心网，以及组网/虚拟化/编排/自动化/运维/分析/AI/边缘计算等。

表 5 电信行业开源基金会

	LFN	ONF	OCP	TIP
会员	111	85	50	500+
项目	9	12	19	包括接入、回传、核心
注册地	美国	美国	美国	美国

数据来源：公开资料整理，2020 年 7 月

我国运营商有一定投入意愿，尚处于跟随状态。我国运营商、设备商、互联网企业积极参与 LFN、OCP 等电信开源组织，中国移动参与 O-RAN 开源生态，作为重要贡献者助力 O-RAN 发布第一版开源软件代码，并担任 O-CU 和 DOC 项目技术领导者(PTL)职位；中国电信明确提出在网络重构过程中优选开源技术，已在主流开源社区建立了影响力，成功入选 OpenStack 黄金会员；中国联通参与 CORD 项目（ONF 组织推动的开源边缘计算的项目之一）。我国运营商和厂商探索主导自主开源生态，2017 年 3 月，中国移动的 Open-O 项目和 AT&T 的 Open-ECOMP 合并，成立开放网络自动化平台（ONAP）项目。

（三）政府采购行业发展开源看重公开透明

政府采购行业信息系统的特点是信息系统建设费用高昂，且政府各部门不互通共享，资源利用率低，政府部门信息科技能力不高。政府采购行业发展开源看重公开透明，一方面开源可以有效解除闭源软件绑定，避免单一商业软件长期锁定，另一方面开源代码公开透明，可以实现多部门复用，从而有效降低成本，提升资源利用率。

全球政府采购行业利用市场强制牵引作用带动开源产业发展。全球政府采购行业开源投入有限，主要利用市场强制推进开源应用，建立配套开源配套设施，通过政府采购市场调动开源生态。**在利用市场强制推进开源应用方面，美国**联邦源代码政策提高政府代码复用率，降低政府采购成本，联邦政府每年在软件上花费数十亿美元，并且部门之间采购的软件存在重叠，因此美国联邦源代码政策开展 2016 年

试点项目，规定美国政府各部门每年采购的软件中 20%的代码需开源，供政府部门内重复使用；**韩国**政府采用 OpenOS 降低对闭源操作系统的使用，拟在 2026 年前让所有公共机构和地方政府采用 OpenOS 系统，有效减少采购商业操作系统以及操作系统技术支持方面的开支；**英国**政府在 2019 年发布的最新版《数字服务标准》第 12 条要求政府部门公开所有新的代码，并选择合适的许可证开源，英国政府认为公共服务是由公共资金建造的，因此这部分涉及的代码应该提供给人们共享和重复利用，同时提高政府部门的代码重复利用率，避免重复工作并降低整个政府的成本。积极布局开源领域投入。**在建立开源配套基础设施方面**，美国为推动政府采购行业建立开源生态，自建代码托管平台，托管政府采购软件领域的开源项目，同时建立配套打分机制，帮助政府部门选择和复用，开源代码扫描平台，保证开源软件引入过程中的风险管理。

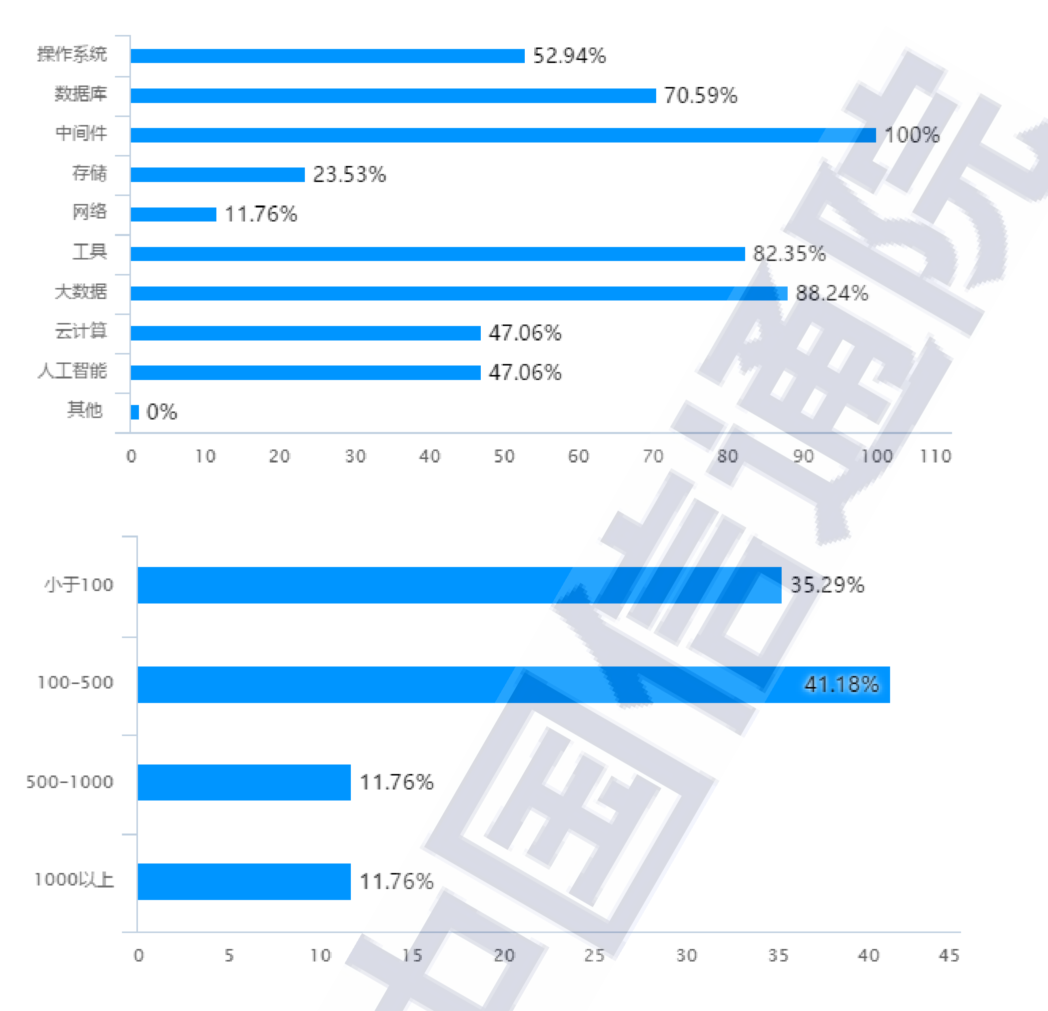
我国政府采购行业积极探索开源合规使用。我国政府采购行业侧重开源使用管理，对于 Linux 操作系统的采购要求“采用 GNU 通用公共许可，详细说明所投产品的基础 linux 版本软件掌握程度，对原始代码的阅读理解程度、注释等”，其它领域软件侧重摸清是否基于开源软件，对于虚拟化及虚拟化管理软件，要求“明确采用开源代码云计算社区版本，经测试和二次开发后，以发行版的形式将软件产品和服务提供给用户，包括计算、存储、网络虚拟化以及虚拟化管理功能”。

（四）金融机构开源看重产业创新力和市场布局

金融行业开源动机总体分为两类，一是看重开源产品的创新度，满足金融机构面临业务场景的新需求，二是金融机构信息科技部门逐渐转型，探索用开源模式建立金融服务生态。

全球金融机构开源协同模式已经形成。金融行业逐步从使用开源转向开放共享，金融机构积极投入开源生态，建立具有行业属性的开源基金会促进产业协同，完善产业链相关配套。金融机构逐步探索开源模式，受开放银行、金融科技大的发展背景影响，金融机构主动探索自发开源模式，摩根大通作为美国最大的金融服务机构之一在 Github 上发布 Quorum 区块链项目代码，高盛将历时 14 年开发的用于帮助用户访问和分析财务数据库的 Alloy 平台通过 FINOS 社区开放给华尔街。金融行业开源协同机制已经建立，2016 年金融科技开放源码基金会（Fintech Open Source Foundation）成立，其核心董事会成员来自花旗集团、摩根大通集团、红帽、GitHub 等企业，FINOS 是全球首个专注金融领域的开源基金会，2020 年与 Linux 基金会建立合作，目前基金会覆盖不同组织的开发者、服务商、科技公司和金融机构等，会员数超过 30 个，孵化项目 11 个，聚集行业 300 多个开源贡献者。

我国金融机构使用开源软件增多。我国金融机构主要以开源用户的身份存在，是开源生态的重要参与者，但与国外基金会对接存在监管合规等多重屏障。开源软件使用仍是我国金融机构参与开源的主要模式。我国金融机构已经从购买闭源软件走向使用开源软件，开源技术应用覆盖领域广泛，头部企业开源软件使用数量达到 1000 以上。



数据来源：中国信息通信研究院，2020 年 5 月

图 35 金融行业开源项目应用情况

我国自主开源模式仍在探索。我国金融机构尝试参与开源生态，但仍主要以用户身份存在，民生银行、中信银行、微众银行等已加入 Linux 基金会，2019 年微众银行将其研发的全球第一个联邦学习工业级开源框架 Federated AI Technology Enabler(FATE)捐赠给 Linux 基金会。

六、开源风险问题复杂，开源治理体系正在构建

（一）知识产权合规及安全漏洞风险相对普遍

开源软件可能涉及三类风险:知识产权及合规风险、安全风险、运维和技术风险，其中知识产权及合规风险主要与开源许可证的规定相

关，安全风险主要涉及安全漏洞等问题，运维和技术风险主要指因开源软件的引入导致的开发运维投入量大、技术人员要求高等问题。

1.开源知识产权及合规风险

除法律法规的保护外，开源软件的作者或权利人主要是通过开源许可证对其知识产权进行许可与约束。若开源软件使用者未依照相应的开源许可证来使用开源软件，将可能侵犯开源软件的作者或权利人的知识产权。

开源许可证涉及的知识产权风险较为复杂。开源使用方在引入开源软件时，因开源许可证的规定或变动，可能面临知识产权及合规风险，一是可能因许可证的传染性规定被迫开源，如：根据 GPL 许可证的规定，使用依 GPL 开源的软件并涉及到修改和分发，需要将后续修改代码全部开源；二是商业软件是否遵守开源约定未知，如：部分商业软件基于开源进行二次开发后以闭源形式提供给用户，却不遵守开源许可证的署名要求；三是知识产权风险易被忽略，如：BSD、MIT 和 GPL 2.0 等并未包含明确的专利许可条款，许可用户使用软件所包含的相关专利；四是开源许可证之间可能不兼容，如：GPL 开源许可证在 GNU 的网站上详细列出何种开源许可证是否与其兼容[2]；五是开源软件的使用规则存在不确定性，如：2018 年以来多个开源软件开发商（Redis 、MongoDB、Kafka 等）已经对其过去使用的开源许可证进行了修改，Oracle 宣布 2019 年 1 月以后发布的 Oracle Java SE 8 公开更新将不向没有商用许可证的业务、商用或生产用途提供。

[2] https://www.gnu.org/licenses/license-list.en.html#GPLIncompatibleLicenses

热门开源项目开源许可证风险较为普遍。经信通院通过开源治理工具扫描显示，容器运行技术领域（Docker、RKT 和 KATA），Docker 的子项目发现少量使用传染性许可证的开源组件，用户在使用过程中需要关注引入、修改、分发方式，判断可能的违约和被开源风险；容器编排技术领域（Kubernetes、Swarm 和 Mesos），均发现少量使用传染性许可证的开源组件;微服务框架领域（Dubbo、istio 和 Tars），均发现使用传染性许可证的开源组件;DevOps 领域(Jenkins 和 Ansible)，Jenkins 许可证存在的隐含风险需引起关注;无服务架构领域（Openwhisk 和 Kubeless），Openwhisk 许可证存在的传染性组件需引起关注;人工智能领域（TensorFlow、Keras 和 Pytorch），TensorFlow 许可证存在的传染性组件需引起关注;数据库领域，MySQL 许可证存在的传染性组件需引起关注。

2.安全漏洞风险

由于开源软件具有多人协作完成、开源许可证存在免责条款等特性，企业在使用开源软件时必须注意数据安全及隐私风险，若开源软件存有恶意代码、病毒或造成隐私泄露，将给使用者带来较为严重的危害，需要跟踪最新版本，及时修复高危漏洞。

热门开源项目存在一定高危漏洞。容器运行技术领域（Docker、RKT 和 KATA），Docker 的子项目发现少量高危和超高危开源组件漏洞;容器编排技术领域（Kubernetes、Swarm 和 Mesos），Mesos 项目发现超高危和高危漏洞数量较多;微服务领域（Dubbo、istio 和 TARS），均发现高危漏洞;DevOps 领域（Jenkins 和 Ansible），Jenkins 发现超高

危漏洞和高危漏洞;无服务器架构领域（Openwhisk 和 Kubeless）开源组件漏洞情况均需引起关注;人工智能领域，TensorFlow（TensorFlow、Keras 和 Pytorch）漏洞数量较多，风险等级较高;数据库领域，MySQL 发现中危漏洞。

（二）开源法律和知识产权环境推动开源良性发展

全球开源法律及知识产权相关实体机构兴起。开源许可协议规则制定权、完善的知识产权法律服务和知识产权保护制度的建立共同为开源软件发展提供了良好的法律环境。OSI从开源软件许可协议入手，结合证明商标，确定了开源许可协议标准，通过教育、协作和基础设施来维护社会中的软件自由，管理开源定义，防止开源运动固有的理想和精神的滥用；SFLC为客户提供开源法律咨询服务，提供自由和开放源码软件项目受影响的所有法律领域的专业知识给客户，包括版权、专利、商标和非盈利治理；OIN是全球最大的专利保护社区，成立时获得了谷歌、IBM、NEC、飞利浦、索尼、SUSE 和丰田等业内企业的大力支持，拥有3200多个会员和1300多项全球专利与应用，OIN专利许可和会员的专利交叉许可对所有OIN社区会员免费开放。

开源许可证有效保证开源项目版权持有人的权利，开源许可证明确开源软件的版权持有人通过许可证，授予用户可以学习、使用、修改开源软件，并向任何人或为任何目的分发开源软件的权利。目前全球开源许可证上千种，大致可以分为四类，开放型开源许可证（Permissive License，如：MIT、BSD）、弱传染型开源许可证(Weak Copyleft License，如：LGPL 2.1)、传染型开源许可证(Copyleft

License，如：GPL 2.0)、强传染型开源许可证(Strong Copyleft License，如：AGPL 3.0)。目前通过OSI认证的开源许可证共有105个，FSF认证的开源许可证157个；各国纷纷制定适合本国的开源许可证，欧盟制定的EUPL，以22种欧洲语言开发，且有将近2万个开源项目使用欧盟公共许可证。根据WhiteSource Software报告显示，67%的开放源码组件使用开源许可证，相比去年增长3%。

（三）开源治理工具加速企业开源治理体系构建

全球开源治理工具经历多次更新换代。开源治理工具主要以开源组成和安全性分析为主，通过扫描开源软件梳理开源组件信息、开源许可证信息、开源安全漏洞信息等帮助用户有效降低开源风险，全球目前主流开源治理工具厂商大多起源于国外，客户遍布全球且占据我国大部分市场份额。国外如 BlackDuck、X-RAY 等开源治理工具大多侧重开源组成识别功能，识别原理按照对识别对象的颗粒度不同大致分为开源组件级别识别和开源文件及代码片段级别，侧重开源组成识别。

我国安全厂商探索开源治理工具。近几年国内出现了许多开源治理工具，从技术层面来看，国内目前市场上的开源治理工具与国外此类工具的技术基本保持一致，从发展层面来看，国内开源治理工具处于快速发展阶段，在扩大国内市场的同时也在积极开拓国际市场。国内开源治理工具厂商多由安全厂商转型，如奇安信开源卫士和棱镜七彩FossEye等。

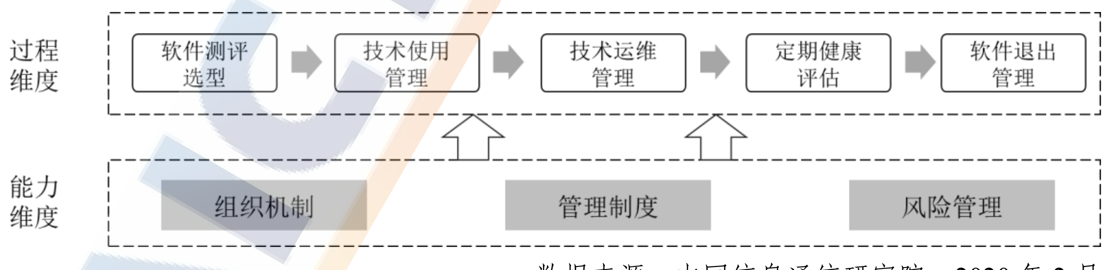
（四）开源治理模式逐步落地

全球开源企业组建开源管理办公室统筹管理。根据 Linux 基金会开源办公室调查报告显示，在 2,700 名研究参与者中，超过一半（52%）拥有正式或非正式开源项目办公室或正在规划创建开源管理办公室。**谷歌**于 2004 年在内部成立开源项目办公室，目的是为了解决使用开源软件带来的许可证和代码的合规问题，办公室的重要原则之一就是帮助其员工使用开源项目和参与开源生态。**Twitter** 于 2010 年左右发现代码许可和法律审查与开发者对外贡献代码之间的平衡导致效率低下，公司决定聘用开源项目经理并创建开源项目办公室，通过引入工具、优化流程等方式简化步骤，实现了开源使用与合规之间的平衡。该办公室目前拥有 15 名成员，负责跟踪公司范围内所使用的开源项目状况，服务于 7.2 万员工和约 2000～4000 个的开源项目。

我国互联网企业关注自发开源治理。腾讯内部成立开源管理小组，该组织经腾讯技术管理委员会授权，由腾讯研发管理职责部门牵头腾讯法务、合规、专利、安全等相关部门，整合为开源管理小组，在开源流程、安全、风险、建议方面对腾讯业务提供服务。在腾讯技术管理委员会的授权下牵头设立了“腾讯开源联盟”，由不同业务的技术专家、负责人、技术领袖组成开源联盟组委会和专家团，在开源文化、开源经验、开源活动等方面对开源项目施以指导和帮助。

出于安全要求，我国传统行业用户率先探索开源引入治理。农业银行、浦发银行、太平洋保险、中信银行等均已构建成熟开源治理体系，从研发、运维双向推动。**研发侧严控引入，把控开源软件风险，**

相比于传统商业软件，开源软件数量更多、问题更为复杂，研发侧有必要在引入开源软件或代码时，严格把控风险，实现开源使用的“可控可溯”。组织机制方面，明确企业开源治理战略，制定配套的开源治理组织架构或开源治理分工，统筹规划和推动企业开源治理工作。管理制度方面，制定相关制度对开源软件进行统一管理，对开源软件的引入、使用、更新、退出的全流程管理做出明确规范，建立开源软件全生命周期的风险管控机制。支撑平台方面，建设配套开源软件管理支撑平台，实现流程管理、社区信息抓取、软件台账、漏洞跟踪、软件仓库等多项功能，有效提高开源软件管理效率；**运维侧持续投入，保证安全稳定运行，**相比于传统商业软件，大多数开源软件缺少付费的运维支持服务，需要本机构投入更多人力物力持续维护。运维分工方面，按照开源软件不同的使用范围和影响程度进行级别划分，并落实后期维护的主体责任，名单管理方面，依据企业内部应用和维护开源软件的实际情况，制定开源软件白名单/黑名单，定期跟踪名单中开源软件的信息变动情况，及时进行反馈和更新。



数据来源：中国信息通信研究院，2020 年 2 月

图 36 开源治理架构图

七、开源生态未来发展趋势与建议

（一）开源生态未来发展趋势

开源从个人行为逐渐发展成为企业行为，开源虽起源于个人行为，但由于开源的协作模式和产品特点，影响商业产品的市场格局，企业层面逐渐借助开源模式实现市场布局，企业层面通过主动布局开源，减低边界成本，引导事实标准，改变市场竞争格局，同时吸纳多方参与，激发产品创新，满足用户多场景需求；**国内逐步主动布局基础软件领域开源生态，**国内早期开源生态发展最早集中在应用侧开发软件领域，虽开源项目数量百万级别，但具有国际影响力的开源项目不足，近年来国内企业逐渐侧重基础软件领域开源项目布局，在操作系统、数据库、中间件等领域涌现多个开源项目，不乏国际基金会的顶级开源项目。

基金会与联盟开源运营呈现多态发展趋势。开源联盟组织将持续推进与企业的开源运营合作，我国开源基金会逐步形成稳定流程机制，国内开源联盟组织相对灵活，覆盖主要技术领域，可借助联盟标准化与行业推广优势，推动我国自发开源项目应用；国际仍以开源基金会作为主要运营载体，为开源项目运营提供有力法律、协作支撑，建立与国内外开源组织、标准化组织建立联动机制，推动开源项目建立生态。

开源风险问题得到关注，开源治理体系逐步建立。开源项目虽最终形成软件、硬件等最终形态，但需要满足开源许可证要求，相比通用软件具有一定的使用范围和规则要求。未来开源风险问题进一步凸显，开源应用情况逐渐透明，开源违约、兼容性、被开源等风险进一步暴露，全球开源违约判例可能进一步增加，企业内部逐

步建立开源治理体系应对开源风险，通过开源管理机制及平台规避开源风险。

行业开源生态兴起。行业用户在开源生态的角色逐渐发生转变，从开源使用到自发开源发展，金融、工业互联网、电信、政府采购等行业逐渐探索行业内开源生态构建，将企业内部信息建设代码脱敏输出，借助开源公开透明的特点快速迭代，形成满足行业属性的特定开源项目，逐步形成行业开源协作机制，实现行业输出战略布局。

（二）我国开源生态发展建议

企业侧建立稳定的开源模式。我国自发开源企业需要建立稳定的开源商业模式，一是针对国际基金会顶级开源项目，建立社区反馈和联动机制；二是建立自主开源生态，重点在操作系统、数据库、中间件等基础软件领域探索开源。

第三方快速完善开源运营机制。一是国内开源联盟组织持续推进与企业的开源运营合作，借助联盟标准化与行业推广优势，推动我国自发开源项目应用；二是开源基金会形成稳定的决策机制，项目孵化流程，为国内开源项目运营提供有力知识产权托管以及法律、协作支撑。

构建开源治理体系。针对自发开源企业、开源使用企业建立开源软件管理体系，第三方组织需制定开源软件治理的行业标准，通过制定开源软件管理规则，帮助企业规范开源软件的使用和输出，实现企业软件的全覆盖和全流程管理，同时配套建设开源风险检测、开源生

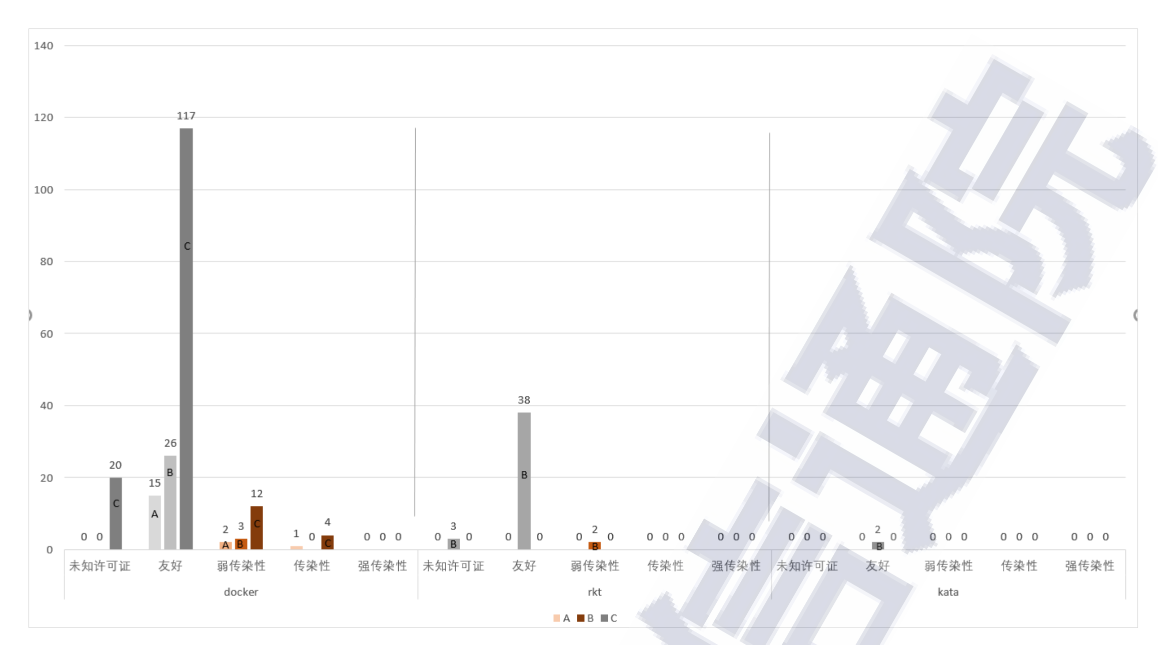
态监测等平台，推动企业落地开源治理体系建设。

附录一：开源软件风险扫描

本白皮书选取开源卫士、BlackDuck 和 FossEye 国内外三款工具对软件源代码进行扫描，设置规则为：以开源组件为单位进行识别和展示，展示三款工具对同一个开源软件的扫描结果，包括开源组件数量，开源许可证分类及数量，开源漏洞分级及数量。其中开源许可证按照传染性的不同分为友好、弱传染性、传染性和强传染性四类，另外未匹配到的许可证类型称为未知许可证；开源漏洞按照严重程度分为低危、中危、高危和超高危四类。因为不同扫描工具对组件颗粒度的定义不同，对开源项目依赖项的探测能力不同导致扫描结果存在差异，本白皮书仅展示自动扫描结果，无人为修改，结果仅供参考。

（一）许可证及合规风险

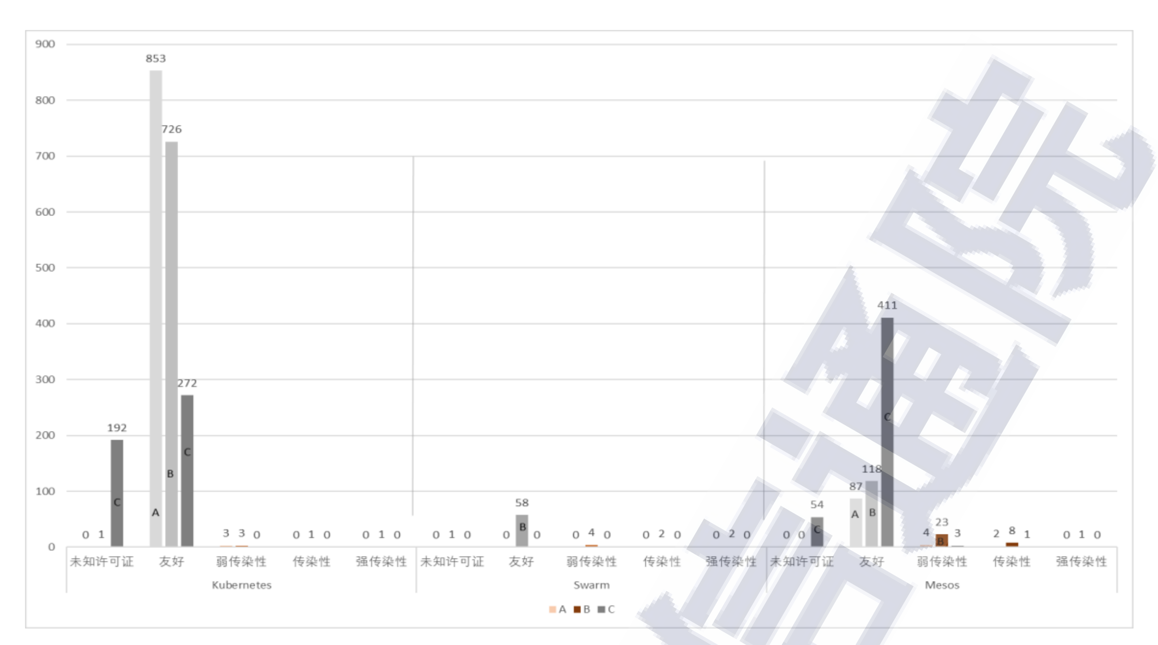
本白皮书对企业选择最多的三个开源容器运行技术（Docker、RKT 和 KATA）进行扫描，结果显示：Docker 的子项目中 A 工具共识别出 1 个组件带有传染性许可证，B 工具共识别出 1 个组件带有传染性许可证，C 工具共识别出 4 个组件带有传染性许可证； RKT 和 KATA 两个项目暂未发现使用传染性许可证的开源组件。



数据来源：中国信息通信研究院，2020 年 4 月

图 37 容器运行技术领域开源许可证风险情况

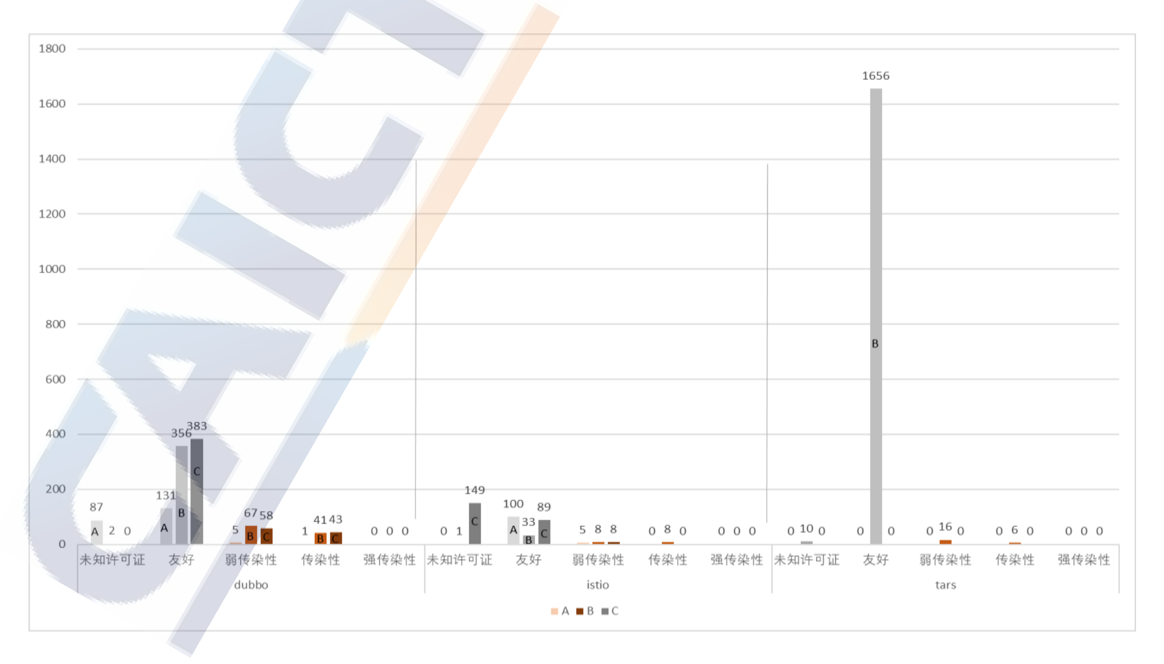
本白皮书对企业选择最多的三个开源容器编排技术（Kubernetes、Swarm 和 Mesos）进行扫描，结果显示：Kubernetes 项目中 B 工具共识别出 1 个开源组件带有传染性许可证，1 个开源组件带有强传染性许可证；swarm 项目中 B 工具共识别出 2 个开源组件带有传染性许可证，2 个开源组件带有强传染性许可证；mesos 项目中 A 工具识别出 2 个开源组件带有传染性许可证，B 工具识别出 8 个开源组件带有传染性许可证，1 个开源组件带有强传染性许可证，C 工具识别出 1 个开源组件带有传染性许可证。



数据来源：中国信息通信研究院，2020 年 4 月

图 38 容器编排技术领域开源许可证风险情况

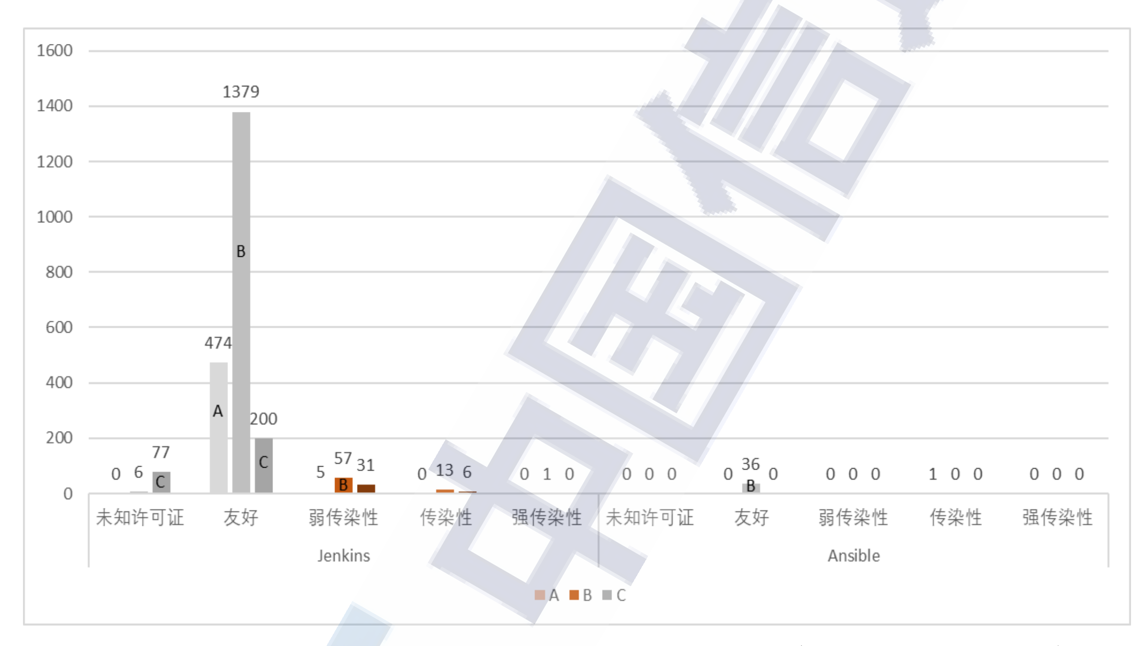
本白皮书对企业选择最多的三个开源微服务框架技术 （Dubbo、istio 和 Tars）进行扫描，结果显示：Dubbo 项目中，A 工具共识别出 1 个开源组件带有传染性许可证，B 工具共识别出 42 个开源组件带有传染性许可证，C 工具共识别出 43 个开源组件带有传染性许可证；istio 项目中，B 工具共识别出 8 个开源组件带有传染性许可证；Tars 项目中，B 工具共识别出 6 个开源组件带有传染性许可证。



数据来源：中国信息通信研究院，2020 年 4 月

图 39 微服务框架领域开源许可证风险情况

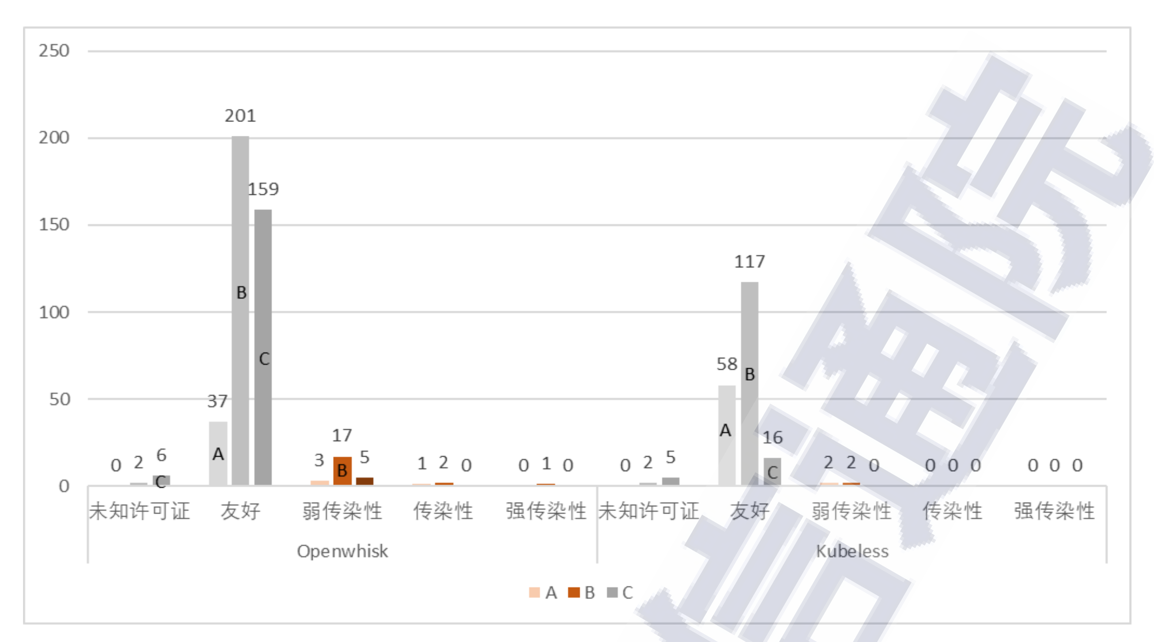
本白皮书对企业选择较多的 2 个 DevOps 领域开源软件（Jenkins 和 Ansible）进行扫描，结果显示：Jenkins 项目中，B 工具共识别出 13 个开源组件带有传染性许可证，1 个开源组件带有强传染性许可证，C 工具识别出 6 个开源组件带有传染性许可证；Ansible 项目三款工具均未检测出带有传染性开源许可证的开源组件。



数据来源：中国信息通信研究院，2020 年 4 月

图 40 DevOps 领域开源许可证风险情况

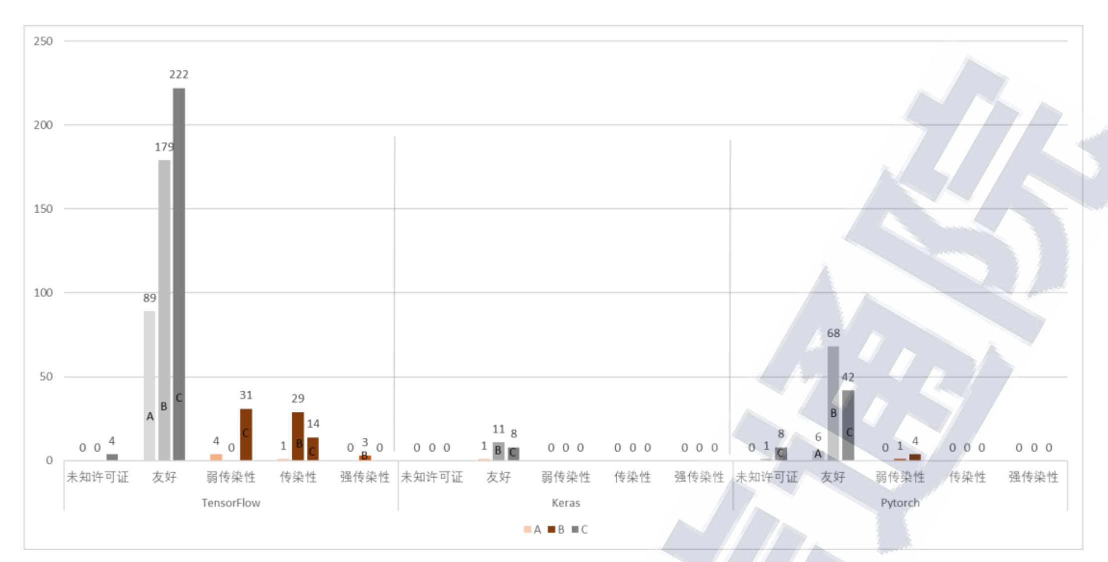
本白皮书对企业选择较多的 2 个无服务架构领域开源软件（Openwhisk 和 Kubeless）进行扫描，结果显示：在 Openwhisk 项目中，A 工具识别出 1 个开源组件带有传染性开源许可证，B 工具识别出 2 个开源组件带有传染性开源许可证，1 个开源组件带有强传染性开源许可证。



数据来源：中国信息通信研究院，2020 年 4 月

图 41 无服务器架构领域开源许可证风险情况

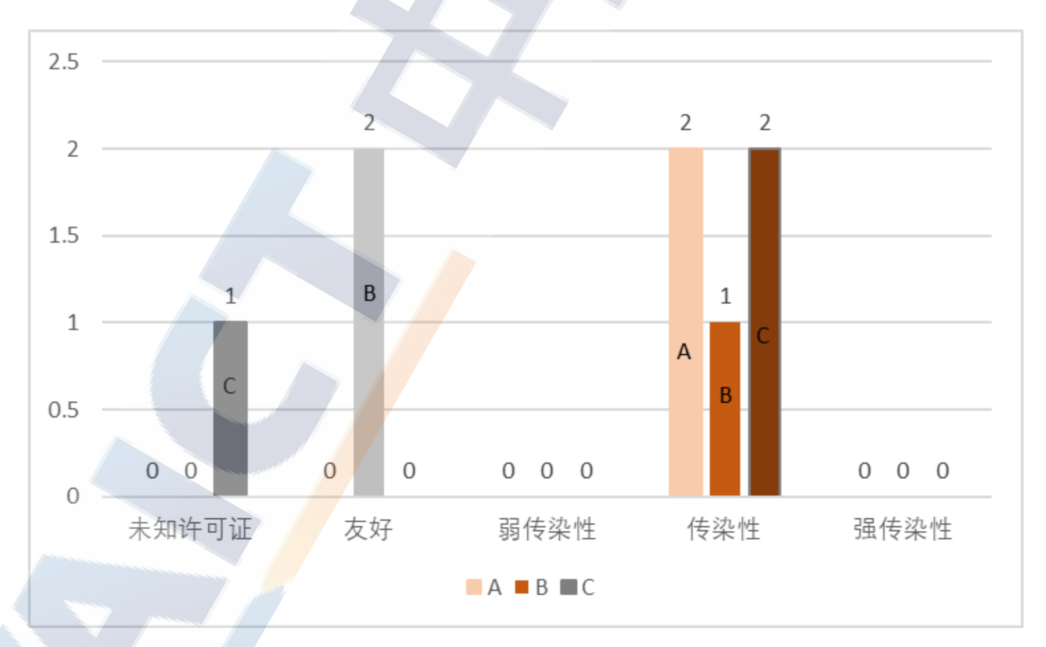
本白皮书对企业选择较多的 3 个人工智能领域开源软件（TensorFlow、Keras 和 Pytorch）进行扫描，结果显示：TensorFlow 项目中，A 工具识别出 1 个开源组件带有传染性开源许可证，B 工具识别出 29 个开源组件带有传染性开源许可证，3 个开源组件带有强传染性开源许可证 C 工具识别出 14 个开源组件带有传染性开源许可证；Ketas 项目中，三款工具均未检测出带有传染性开源许可证的开源组件；Pytorch 项目中，三款工具均未检测出带有传染性开源许可证的开源组件。



数据来源：中国信息通信研究院，2020 年 4 月

图 42 人工智能领域开源许可证风险情况

本白皮书对企业选择较多的 1 个数据库领域开源软件 MySQL 进行扫描，结果显示：MySQL 项目中，A 工具识别出 2 个开源组件带有传染性开源许可证，B 工具识别出 1 个开源组件带有传染性开源许可证，C 工具识别出 2 个开源组件带有传染性开源许可证。



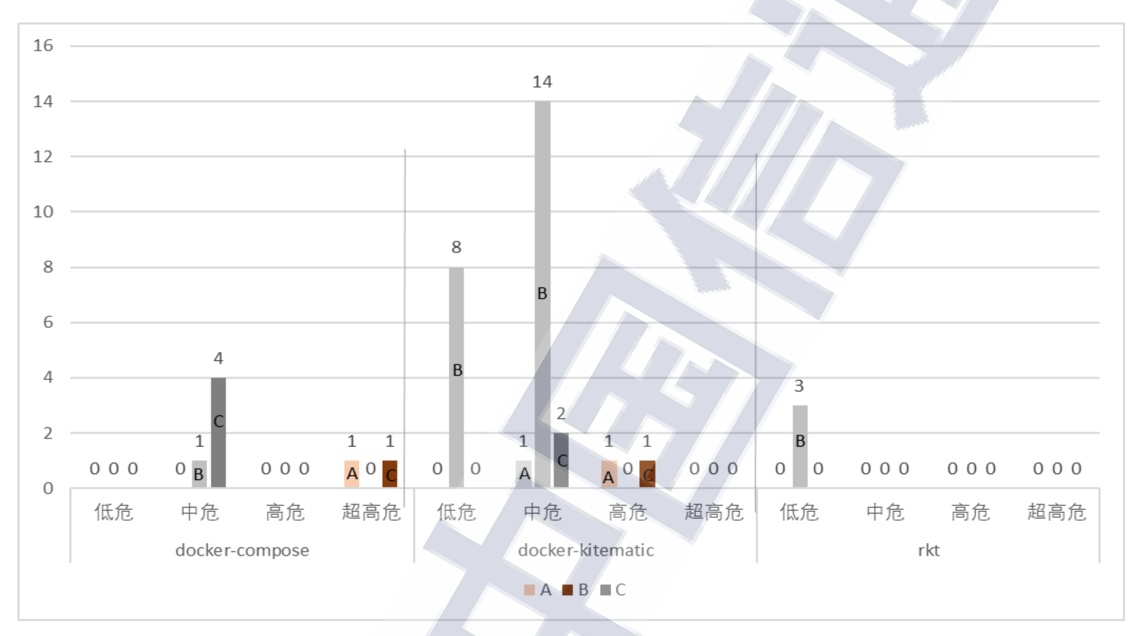
数据来源：中国信息通信研究院，2020 年 4 月

图 43 数据库领域开源许可证风险情况

（二）安全漏洞风险

本白皮书对企业选择最多的三个开源容器运行技术（Docker、

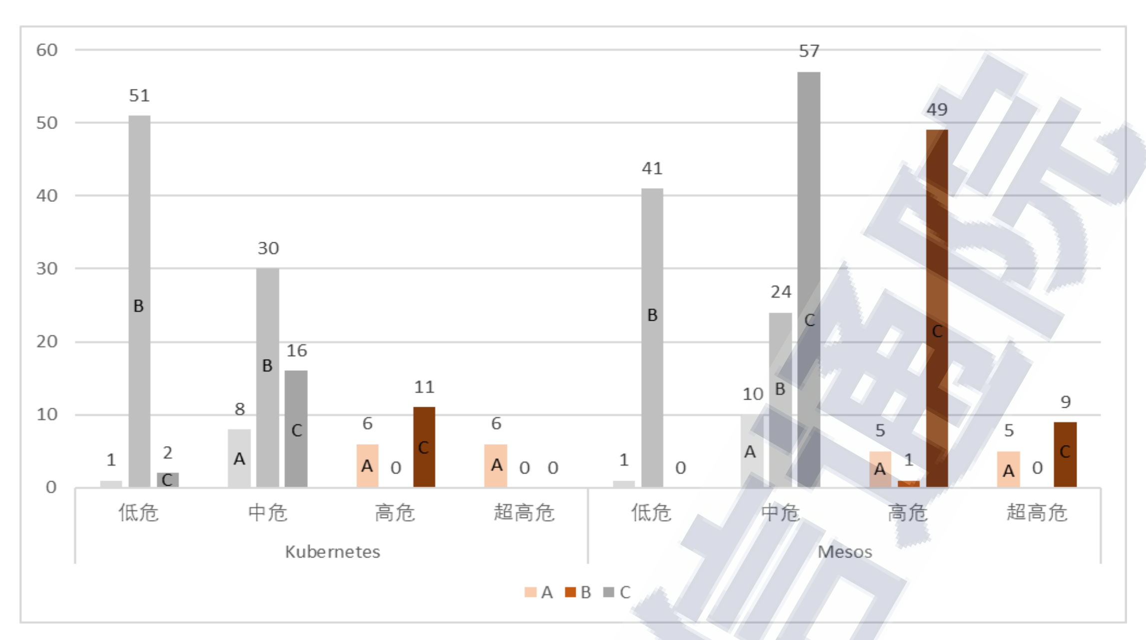
RKT 和 KATA）进行扫描，结果显示：Docker 的子项目中 A 工具共识别出 1 个超高危漏洞、1 个高危漏洞和 1 个中危漏洞，B 工具共识别出 15 个中危漏洞和 8 个低危漏洞，C 工具共识别出 1 个超高危漏洞、1 个高危漏洞和 6 个中危漏洞；RKT 项目中，B 工具识别出 3 个低危漏洞；KATA 项目暂未发现开源漏洞。



数据来源：中国信息通信研究院，2020 年 4 月

图 44 容器运行技术领域开源漏洞风险情况

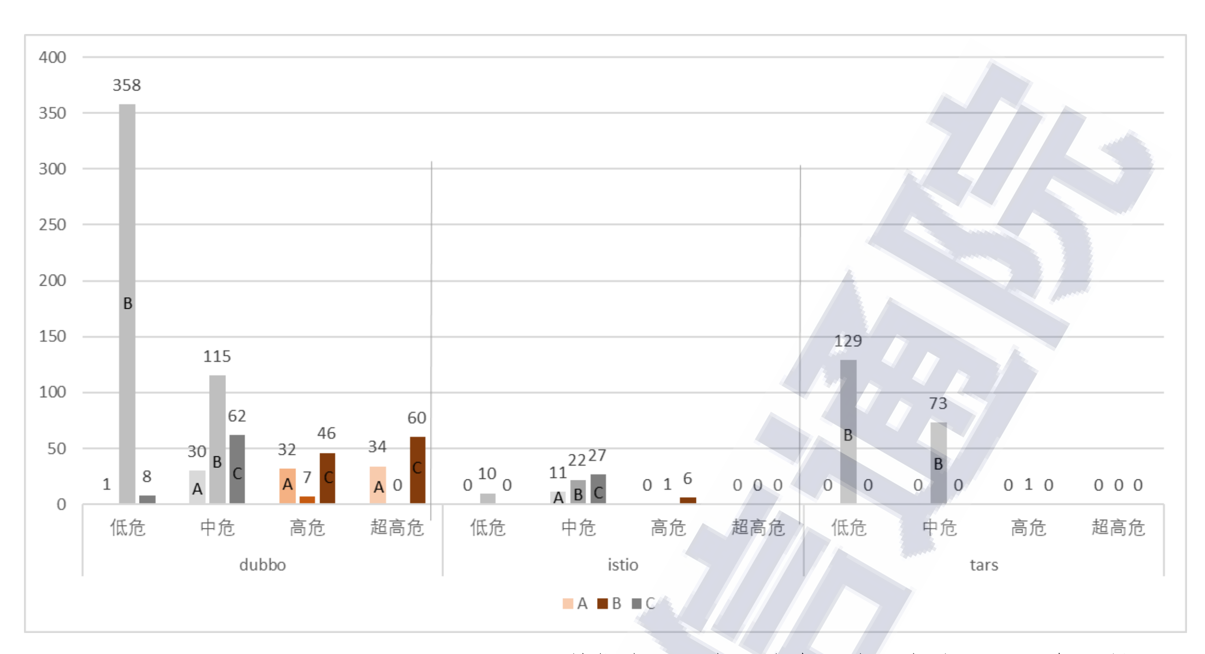
本白皮书对企业选择最多的三个开源容器编排技术（Kubernetes、Swarm 和 Mesos）进行扫描，结果显示：Kubernetes 项目中 A 工具共识别出 6 个超高危漏洞、6 个高危漏洞、8 个中危漏洞和 1 个低危漏洞，B 工具共识别出 30 个中危漏洞和 51 个低危漏洞，C 工具共识别出 11 个高危漏洞、16 个中危漏洞和 2 个低危漏洞；swarm 项目中未发现开源漏洞；Mesos 项目中 A 工具识别出 5 个超高危漏洞、5 个高危漏洞、10 个中危漏洞和 1 个低危漏洞，B 工具识别出 1 个高危漏洞、24 个中危漏洞和 41 个低危漏洞，C 工具识别出 9 个超高危漏洞、49 个高危漏洞和 57 个中危漏洞。



数据来源：中国信息通信研究院，2020 年 4 月

图 45 容器编排技术领域开源漏洞风险情况

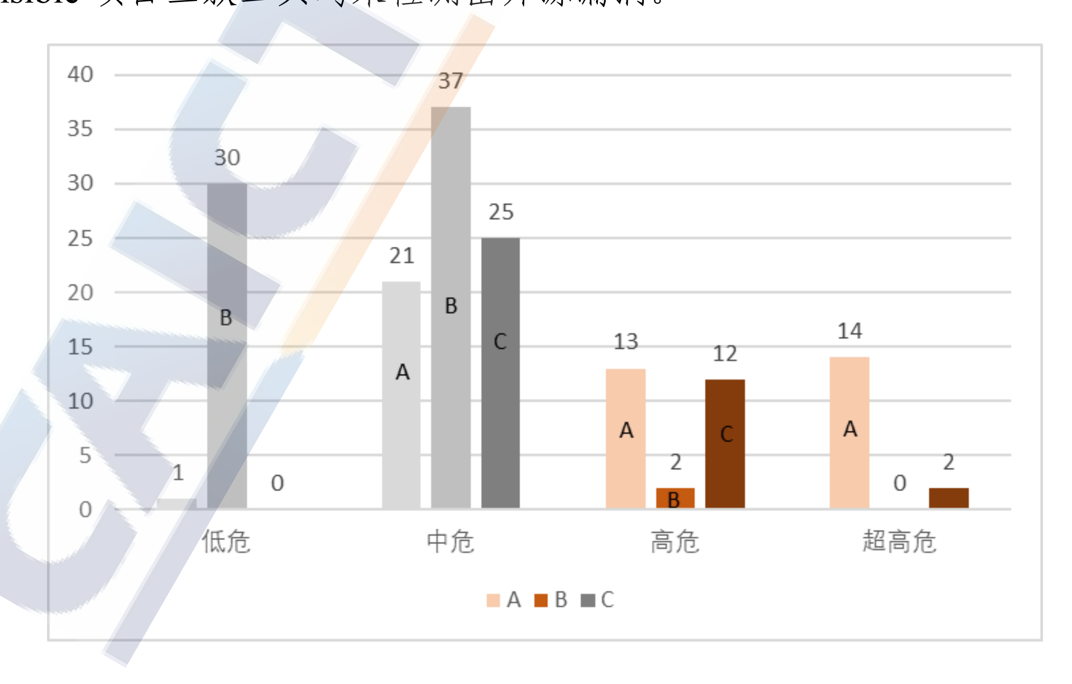
本白皮书对企业选择最多的三个开源微服务框架技术 （Dubbo、istio 和 TARS）进行扫描，结果显示：Dubbo 项目中，A 工具共识别出 34 个超高危漏洞、32 个高危漏洞、30 个中危漏洞和 20 个低危漏洞，B 工具共识别出 7 个高危漏洞、115 个中危漏洞和 358 个低危漏洞，C 工具共识别出 60 个超高危漏洞、46 个高危漏洞、62 个中危漏洞和 8 个低危漏洞；istio 项目中，A 工具识别出 11 个中危漏洞，B 工具共识别出 1 个高危漏洞、22 个中危漏洞和 10 个低危漏洞，C 工具共识别出 6 个高危漏洞和 27 个中危漏洞；TARS 项目中，B 工具共识别出 73 个中危漏洞和 129 个低危漏洞。



数据来源：中国信息通信研究院，2020 年 4 月

图 46 微服务领域开源漏洞风险情况

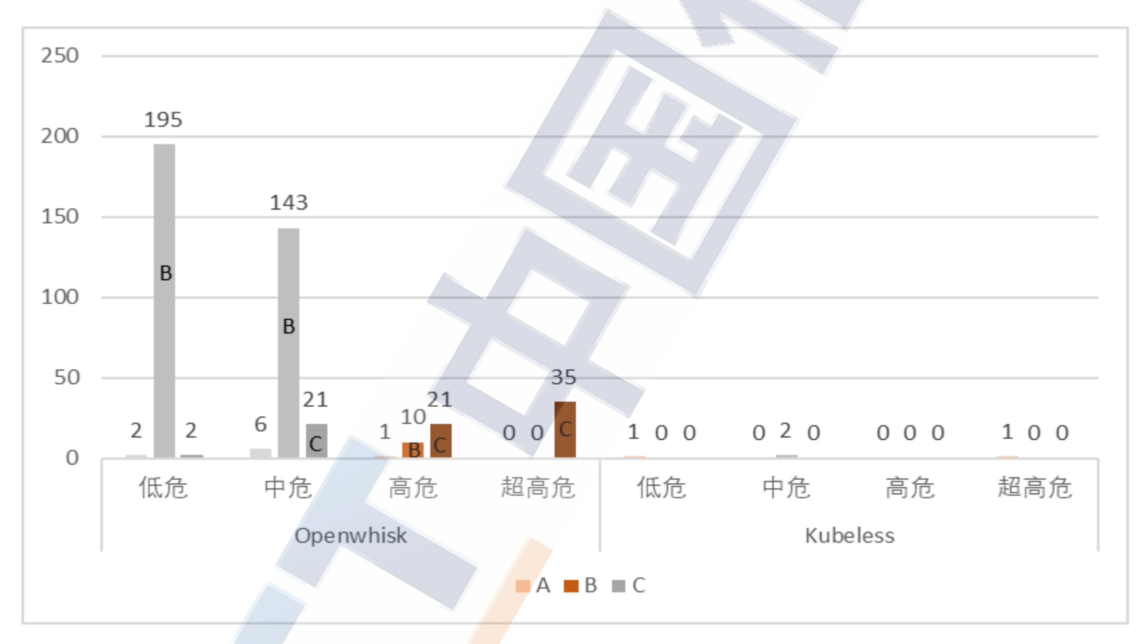
本白皮书对企业选择较多的 2 个 DevOps 领域开源软件（Jenkins 和 Ansible）进行扫描，结果显示：Jenkins 项目中，A 工具共识别出 14 个超高危漏洞、13 个高危漏洞、21 个中危漏洞和 1 个低危漏洞，B 工具共识别出 2 个高危漏洞、37 个中危漏洞和 30 个低危漏洞，C 工具共识别出 2 个超高危漏洞、12 个高危漏洞和 25 个中危漏洞；Ansible 项目三款工具均未检测出开源漏洞。



数据来源：中国信息通信研究院，2020 年 4 月

图 47 DevOps 领域开源漏洞风险情况

本白皮书对企业选择较多的 2 个无服务架构领域开源软件（Openwhisk 和 Kubeless）进行扫描，结果显示：在 Openwhisk 项目中，A 工具识别出 6 个中危漏洞和 2 个低危漏洞，B 工具识别出 10 个高危漏洞、143 个中危漏洞和 195 个低危漏洞，C 工具共识别出 35 个超高危漏洞、21 个高危漏洞、21 个中危漏洞和 2 个低危漏洞；在 Kuberless 项目中，A 工具识别出 1 个超高危漏洞和 1 个低危漏洞，B 工具识别出 2 个中危漏洞。

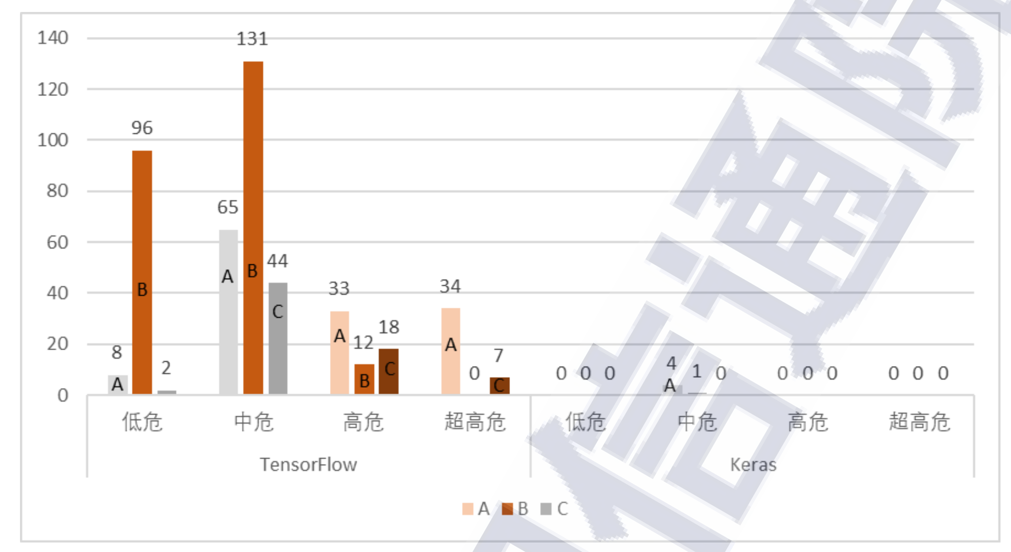


数据来源：中国信息通信研究院，2020 年 4 月

图 48 无服务器架构领域开源漏洞风险情况

本白皮书对企业选择较多的 3 个人工智能领域开源软件（TensorFlow、Keras 和 Pytorch）进行扫描，结果显示：TensorFlow 项目中，A 工具识别出 34 个超高危漏洞、33 个高危漏洞、65 个中危漏洞和 8 个低危漏洞，B 工具识别出 12 个高危漏洞、131 个中危漏洞和 96 个低危漏洞，C 工具识别出 7 个超高危漏洞、18 个高危漏洞、44 个中危漏洞和 2 个低危漏洞；Ketas 项目中，A 工具识别出 4 个中

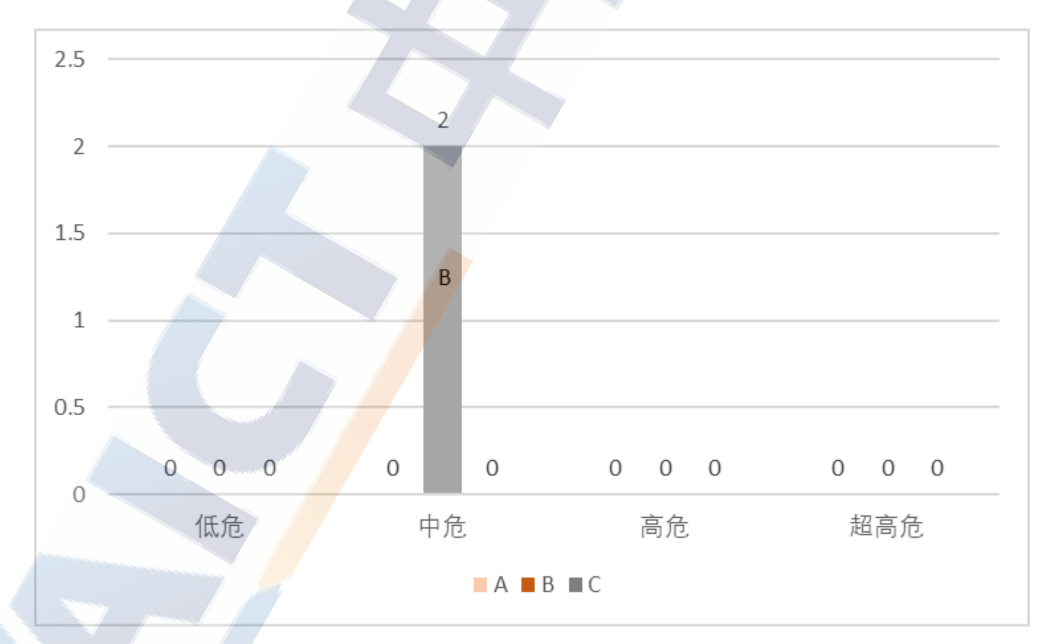
危漏洞，B 工具识别出 1 个中危漏洞；Pytorch 项目中，三款工具均未检测出开源漏洞。



数据来源：中国信息通信研究院，2020 年 4 月

图 49 人工智能领域开源漏洞风险情况

本白皮书对企业选择较多的 1 个数据库领域开源软件 MySQL 进行扫描，结果显示：MySQL 项目中， B 工具识别出 2 个中危漏洞。



数据来源：中国信息通信研究院，2020 年 4 月

图 50 数据库领域开源漏洞风险情况

附录二：企业开源治理案例

（一）浦发银行开源治理案例

1. 概述

伴随着金融行业数字化转型的强烈需求，越来越多的银行应用系统会构建在开源软件之上，并享受其带来的定制灵活、功能丰富、迭代快速、人才资源集中等好处。但同时，开源软件有别于商用软件，其安全性、可靠性、可维护性以及许可遵从都会给银行科技建设带来新的挑战。银行需要在技术上、社区上、法务上全面评估和把控开源软件使用风险。浦发银行根据自身特点建设了开源技术治理体系，为未来自主、高效、安全地使用开源软件提供技术和制度上的保证。

2. 开源治理体系建设

浦发银行开源治理体系是一套帮助浦发银行安全、合规、可靠、高效地评估和使用开源软件、管理开源软件资产、把控开源软件使用中的安全风险的方法论和实践。主要包含以下五部分内容:

（1）开源治理的配套组织机制。指组织架构或开源治理分工，制定开源治理战略和开源治理流程，统筹规划和推动企业开源治理工作，包括开源管理、软件维护、安全支持、法律支持等。

浦发银行内部组建开源治理组织架构，发布开源治理规程。目前，浦发银行开源治理组织架构分为：开源治理团队、开源专业团队、开源安全团队、开源法务团队（待建）。

- 开源治理团队：主要负责制定和执行开源软件应用管理规则及开源软件日常管理工作。同时，开源治理团队熟悉开源软

件社区的各种指标含义和获取方法，有效保证了开源软件社区信息获取和评估的效率。

（2）开源治理的配套管理流程制度。制定相关管理制度对开源软件的合规使用进行管控，包括引入、使用、风险管理、更新、退出的全生命周期的流程管理。

（3）开源软件评估评价机制。一套适合于金融行业业务和管理特点的开源软件评估评价方法，用于指导开源软件在银行的引入和选型。

浦发银行依据 E- OSMM (Enterprise Open Source Maturity Model) 模型以及华为开源治理的成功经验，结合银行行业特色以及浦发银行自身需求，形成了一套开源软件评估体系。

（4）开源软件治理支撑平台。一个用于支撑开源软件治理的平台系统，是整个开源治理工作高效运行的技术保障。

开源治理流程在源头上控制了高风险开源软件版本的引入，有效收敛了浦发银行应用开源软件的种类和版本，筛查并拒绝了社区发展前景不佳的开源软件。对于已经投入使用的开源软件，也能够持续跟踪防范其安全风险。

（5）金融行业开源技术应用社区。一个非盈利性的组织，旨在通过信息共享，推动开源技术和软件在金融行业内安全可靠的使用。

3. 总结

浦发银行从无到体系化了开源治理工作，并和行内软件项目流程相结合实现了落地运行，形成了包括相应工具平台在内的工作机制。

同时，浦发银行发起成立了金融行业开源技术应用社区，社区成员多为金融机构。浦发银行面向社区内部开源了开源治理平台，有效帮助社区成员快速获取开源治理能力，解决了金融行业开源软件管理痛点，促进行业内开源软件安全可靠使用。浦发银行凭借这套开源治理体系和相应实践，获得了中国通信标准化协会（CCSA）的开源治理能力认证，成为首批获得该认证的金融机构。同时，也获得了 OSCAR（云计算开源产业联盟）尖峰开源用户奖。后续浦发将基于行内开源治理需求和实践，继续完善开源治理研究。

（二）中信银行开源治理案例

1、概述

随着开源软件漏洞频发、监管要求的相继出台，中信银行对开源治理工作也更加重视。2020 年 3 月发布开源治理细则，组建开源治理团队，对开源软件全生命周期进行管控。目前中信银行按照先梳理，再治理的整体思路，逐步建立开源治理体系，最终实现开源软件的分级分类管理、统一版本、统一发布和安全可控。

2、开源治理团队的角色划分及职责如下:

软件开发中心作为开源软件的实施部门，下设

开源软件使用员：负责提出开源软件管理全流程的申请，并参与评审；负责开源软件管理全流程测评方案和计划的制定实施，并参与评审；负责向开源软件分类管理员报送开源软件的使用情况及服务供应商的技术支持情况。

开源软件分类管理员：负责制定和发布开源软件管理全流程相关

模版；负责参与开源软件主管部门组织的评审；负责组织开源软件引入的测评工作，根据开源软件类型，从专家资源池中选择相应专家，对《开源软件测评方案和计划》进行评审；负责组织收集和登记所辖开源软件的使用情况、性能和安全问题及服务供应商的技术支持情况。

开源软件归口管理员：作为归口角色向开源软件主管部门提出开源软件管理全流程的申请；负责建立和维护开源软件制品库，做好开源软件、组件的介质管理和版本管理。

开源软件审批团队：由各领域推荐技术专家，共同维护开源软件评审专家资源池。

3、开源软件引入与升级管理：

开源引入分级：依据开源扫描结果，将待引入的开源软件按照使用范围和影响程度进行分级，不同级别的开源软件引入周期不同。

开源引入流程：较低级别的开源软件进行线上会签评审并编写测评报告和试用报告；中高级别的开源软件需要分类管理员组织领域专家对测评计划和测试案例进行线下评审，审核通过后进入试用期，试用期结束后针对开源测评报告和试用报告进行准入评审，并明确自主掌控部门和运维部门。准入评审会议通过后，开源软件分类管理员负责组织编写使用手册和优化建议，开源软件归口管理员负责将安装介质纳入开源软件制品库进行管理，将文档纳入知识库进行管理。

开源软件升级流程：开源软件的大版本视为不同软件，在引入新的大版本时，需要重新进行软件准入流程（需求申请、测评、评审）。对需要二次开发后方可使用的开源软件，开源软件使用员需在引入后

立即提起二次开发流程。

未来，中信银行会在开源治理的道路上不断探索，持续学习业界先进经验，在增强开源管控能力的同时，进一步提升开源影响力、贡献力，拥抱开源，回馈开源。

（三）中国银行开源应用案例

中国银行大数据监控平台基于开源 ZABBIX 用于对各个大数据组件集群集中监控。监控的指标项一部分是从官方指标中挑选的主要指标，一部分是对组件原生指标进行进一步加工后的指标。这些展示一方面可以简要表明集群的状态，另一方面避免了部分指标需要手工命令查询的时间消耗，并且能集中展示，方便运维人员快速查找，同时也可以协助开发人员确定应用程序的性能。

Zabbix-agent 部署在被监控的主机上，负责定期收集各项数据，并发送至 zabbix-server 端，之后 zabbix 会将数据存储到数据库 database 中；使用 Zabbix API 提供的可编程接口获取监控数据、通过 Http 协议获取主机配置信息，一并保存到本地数据库 TiDB 中；后端读取数据并进行分析，构建服务将结果发送至前端，前端发送 Ajax 请求获取响应并展示数据。

（四）中兴开源治理案例

为了满足公司产品研发不断增长的需求，解决提升质量和开发效率的矛盾，大量的开源软件被引入到产品的研发过程以及产品本身之中。为了确保使用开源软件的产品版本对外合规分发，有效的应对和

管控各类风险，中兴通讯制定了一整套的开源软件治理机制。

中兴通讯制定了《开源软件管理规范》作为开源软件治理的纲领性文件。此规范在以下各方面对开源软件在公司内的全生命周期进行了规定。此规范在相应的 IT 工具系统的支撑下，形成了完善的开源软件管理和治理机制。

1、概述

中兴通讯的开源治理主要希望达到的目的是: 管控开源软件的引入，确保产品项目尽量使用主流的、相对成熟的、风险相对较小的开源软件。不允许开发人员随意引入不可靠的开源软件; 公司内使用的同一个开源软件的同一个版本的代码和制品的来源相同。这可以防止产品开发人员从非官方托管地等不可靠的地方下载可能存在病毒等恶意隐患的代码和制品。同时对开源软件严重漏洞的自研修改方案可以快速的在所有产品上生效; 及时发现产品因使用开源软件引入的漏洞并加以治理; 确保产品对外发布时涉及开源软件部分的合规使用和分发。为此，中兴通讯建立了一整套开源软件相关的制度，自研和引入了相关的工具，建立了完善的开源软件管理和治理机制。

2、开源软件的选型和引入

当一个产品项目需要增加某种功能组件，并且考虑通过引入开源软件来实现的时候，必须通过一个开源软件引入流程来完成引入。

首先，产品项目需要进行预研，确定几个可以满足功能与性能要求的备选开源软件以及版本，然后确定其中一个作为选型结果。然后在公司开源软件库中查找，此软件的此版本是否已经在库中存在，如

果已经存在，则不必再走新引入流程。如果此软件此版本尚未在公司开源软件库中存在，则需要向开源软件库提交一个入库申请，附带选型预研结果和测试报告。此申请由公司的开源专家团队进行审批处理。开源专家团队从若干方面因素对所申请的开源软件版本进行评估打分，达到一定分数水平后才批准入库使用。这些评估因素包括：开源软件所使用的开源许可证，漏洞情况，业界采纳度，版本发布周期，开发者社区规模，是否有开源基金会支持等等。

开源软件的版本在通过审批后，由开源软件库从开源软件的官网以及其他可靠托管地下载其源码和/或制品（如 rpm 包，jar 包等等），经过安全扫描后进行存放。产品在后续构建版本时，直接从公司开源库中取用所需开源软件版本的代码和制品。

3、开源软件的同源治理

开源软件在进入开源软件库后，可以供公司内所有产品项目使用。这保证了所有产品项目使用的开源代码和制品都是从同一个可靠来源下载的。避免了各产品项目的研发人员自行从网上下载时取用了不可靠来源导致引入病毒和后门等安全隐患。同时，对开源软件严重漏洞的自研修改方案可以快速的在所有产品上生效。

4、开源漏洞治理

中兴通讯引入了第三方安全漏洞扫描工具，对产品进行定期扫描以及发布前的扫描。发现安全漏洞后在规定的时间内予以评估响应。一旦评估新发现的漏洞对产品有比较重要的影响，就通过升级软件或自研补丁的方式进行修正治理，确保发布出去的产品没有影响产品安

全和用户安全的漏洞。

5、开源软件合规使用和分发

根据美国出口管制条例（EAR）的规定，开源软件原则上不受管辖。但是含有一定秘钥长度的一些指定加密算法的美国原产开源软件需要受管辖及管控。但是可以根据 EAR 742.15(b)(2)的规定，在向美国商务部工业与安全局(BIS)进行备案后来解除管辖。因此，为了合规使用，一个开源软件的版本引入到开源软件库后，需要判断它是否需要向 BIS 备案来解除美国 EAR 的管辖。目前判断一个开源软件是否需要备案的原则为，需同时满足：是公开可获得的源码形式的开源软件；此开源软件为美国的基金会、美国的开源软件社区或美国的公司发起；或发起方不确定，但是有美国人参与，或美国公司参与，或外国人在美国参与的；或无论发起方的国籍还参与人的国籍存在不明确的情况的；此开源软件的出口管制分类编号（ECCN）为 5D002；或者包含了加密算法；或者不确定是否有加密算法。

满足上述条件的开源软件，开源软件库会触发向 BIS 备案的流程来解除 EAR 管辖。

含有开源软件的产品版本分发时会附带一个开源软件声明书，其中包含了此产品所使用的所有开源软件的信息，以符合相关开源许可证的要求。

（五）红帽开源治理案例

随着开源软件在企业中采用的比重越来越大，企业对于开源软件的引入，使用，改造以及安全的管理需求越来越突出。因此，红帽软

件把自己长期专注开源软件生态建设形成的开源软件管理理念，以及多年开源运营及开源项目实施所积累的一整套实践经验分享出来，结合国内开源发展的实际，提出了开源治理的最佳实践框架。

红帽的开源治理最佳实践框架，概括地说，就是围绕一个总体目标愿景，通过三阶段推进实施，在四个领域全方位展开，简称 314 开源治理框架。

在开源治理的总结和实践过程中，针对不同阶段，不同领域，红帽都有相对应的方法，流程或者工具来帮助企业完成相关过程的实施。

红帽把开源治理成熟度分成 0-4，共 5 个级别，来定义开源治理的成熟度，分别是 1）不可见；2）参与；3）规范；4）成熟；5）贡献。

有了整体规划，企业可以逐步展开具体的治理体系建设，进行落地实施。在企业进行开源治理的过程中，往往把重点放在开源技术本身，而忽略了其他一些同样重要的因素。红帽认为开源体系建设是一个统一的过程，建议企业可以从开源管理体系，开源组织体系，开源技术体系和开源文化体系（即我们说的 PPTC）四个领域展开实施。

对于开源管理体系建设，红帽提出了围绕开源技术进行全生命周期管理的理念，即从开源技术的导入，使用，更新，升级，退出各个阶段进行管理。

在开源管理体系建设过程中，通过实际项目开展，我们建立了开源导入的维度模型，从技术针对性、技术先进性、开源社区活跃度、生命力等五个方面进行全面评估，来查看拟采用的开源软件是否有风险，以及如何规避风险，更科学、更有效地来使用这个开源软件。

对于开源组织体系建设，红帽提出了开源管理金字塔模型。

对于开源技术体系建设，红帽建议的方法是建立知识库和开源实验室，通过开源实验室，把内部，外部的专家积累经验沉淀到知识库里。随着开源使用过程的不断积累，以及技术的不断地迭代和演进，企业对开源管理的成熟度也会越来越高。

开源治理是一个逐步迭代的过程，管控风险是很多企业进行开源治理的重要出发点，但是，引领创新才是开源治理的最重要的目标。在开源治理实践过程中，如果没有开源文化体系建设，开源治理往往止步于“管”，难以发挥开源治理的引领作用。红帽坚持上游优先，拥抱社区的，引领开源发展的文化理念，在建立开源社区文化，开源技术生态文化，开源回馈及影响力文化上有很多积累和经验，并开创性提出了创新实验室项目，可以快速帮助客户融入开源技术生态，并建立起自己的开源品牌和影响力，让开源在企业中生根发芽，枝繁叶茂。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300557

传真：010-62304980

网址：www.caict.ac.cn

